CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION

J-6
DISTRIBUTION: A, B, C, J

CJCSI 6731.01B, CH 1
30 August 2006

GLOBAL COMMAND AND CONTROL SYSTEM - JOINT SECURITY POLICY

1. Purpose. This instruction defines the security policy for the Global Command and Control System-Joint (GCCS-J), its strategic servers, and GCCS Top Secret (GCCS-T). This instruction implements DODD 8500.1, "Information Assurance (IA)," and DODI 8500.2, "Information Assurance (IA) Implementation."

2. Cancellation. This instruction supersedes CJCSI 6731.01A, 1 August 2006.

3. Applicability. This instruction applies to the Joint Staff, Services, Defense agencies, combatant commands, and other agencies and organizations that develop, use, or plan to use GCCS-J, its strategic servers, and/or GCCS-T.

4. Policy. GCCS-J is a US system. Warfighters will be provided GCCS-J security policy consistent with US public laws and policy; DOD information security policy; automated information system security policy; defense information warfare policy; and defensive information warfare policy, strategy, and doctrine.

5. Definitions. See Glossary.

6. Responsibilities

a. The Chairman of the Joint Chiefs of Staff is responsible for:

(1) Providing a GCCS-J security policy that supports user requirements and selected solutions.

(2) Identifying the minimum system security requirements for GCCS-J system developers.

(3) Identifying conditions or requirements for entry to various program phases such as operational test, initial operational capability, full operational capability, and system shutdown and termination.

b. The Director for Command, Control, Communications, and Computers (J-6), Joint Staff, supports the Chairman and the Director for Operations (J-3), Joint Staff, in accomplishing the responsibilities set forth in this instruction. The Director, J-6, is responsible for:

(1) Serving as the global GCCS-J designated approving authority (DAA). Enclosure C defines the global GCCS-J DAA's responsibilities.

(2) Appointing a GCCS-J Security Officer (GSO). Enclosure C defines the GSO's responsibilities.

c. The Director, Defense Intelligence Agency (DIA), provides the Joint Staff with GCCS-J systems certification, test, and evaluation (CT&E) support in accordance with this instruction and current DOD certification and accreditation (C&A) guidance. The Director, DIA, is responsible for:

(1) Performing security certification of GCCS-J baseline systems (strategic servers), including security testing of GCCS-J and its components.

(2) Performing GCCS-J security testing with guidance from the Joint Staff/J-3 and Joint Staff/J-6.

(3) Providing day-to-day GCCS-J security advice and consulting to the Joint Staff.

d. The Director, Defense Information Systems Agency (DISA), as the overall systems integrator for GCCS-J, provides the Joint Staff with all GCCS-J systems security integration support following guidance in this instruction. The Director, DISA, is responsible for:

(1) Assisting the Joint Staff in implementing GCCS-J security policy.

(2) Ensuring proper GCCS-J certification can be maintained in the overall systems integration and fielding process.

(3) Providing GCCS-J security operational support to the Joint Staff, Services, and combatant commands.

e. Service Chiefs, combatant commanders, Service components, and Directors of Defense agencies are responsible for:

(1) Appointing an official to serve as the site GCCS-J DAA for the Service Chief, combatant commander, Service component, or agency sites. Enclosure C identifies site GCCS-J DAA responsibilities.

(2) Ensuring the site GCCS-J DAAs appoint site GCCS-J information assurance managers (IAMs) and officers (IAOs) as described in Enclosure C.

(3) Ensuring the site GCCS-J DAAs monitor operational objectives so mission support with minimum response time does not conflict with the security goals of maximum control and minimum risks.

7. Summary of Changes. Change 1 corrects pagination errors produced by electronic signature of CJCSI 6701.01B. Software conflicts between Microsoft Office 2003 and Approve It are in the process of being resolved.

8. Releasability. This instruction is approved for public release; distribution is unlimited. DOD components (to include the combatant commands), other federal agencies, and the public may obtain copies of this instruction through the Internet from the CJCS Directives Home Page--http://www.dtic.mil/cjcs_directives. Copies are also available through the Government Printing Office on the Joint Electronic Library CD-ROM.

9. Effective Date. This instruction is effective upon receipt.

For the Chairman of the Joint Chiefs of Staff:

WALTER L. SHARP
Lieutenant General, USA
Director, Joint Staff

Enclosures:

A – System Classification
B – GCCS Minimum Security Requirements
C – Responsibilities
D – Network Security

E – GCCS-J Security Policy Waiver Authority
F – GCCS Strategic Server Policy
G – GCCS Personal Digital Assistant and Personal Electronic Device Policy
H – GCCS-J Keyboard, Video, Mouse Switch Policy
I – References
GL – Glossary

LIST OF EFFECTIVE PAGES

The following is a list of effective pages for. Use this list to verify the currency and completeness of the document. An "O" indicates a page in the original document.

PAGE	CHANGE	PAGE	CHANGE
1 thru 4	O	E-1 thru E-2	O
i thru iv	O	F-1 thru F-2	O
A-1 thru A-2	O	G-1 thru G-2	O
B-1 thru B-26	O	H-1 thru H-4	O
C-1 thru C-10	O	I-1 thru I-6	O
D-1 thru D-6	O	GL-1 thru GL-17	O

(INTENTIONALLY BLANK)

RECORD OF CHANGES

Change No.	Date of Change	Date Entered	Name of Person Entering Change

(INTENTIONALLY BLANK)

TABLE OF CONTENTS

ENCLOSURE E -- GCCS-J SECURITY WAIVER AUTHORITY

ENCLOSURE H -- GCCS-J KEYBOARD, VIDEO, MOUSE SWITCH POLICY

ENCLOSURE I -- REFERENCES

GLOSSARY

ENCLOSURE A

SYSTEM CLASSIFICATION

1. Mission Overview. The GCCS-J is the DOD joint command and control (C2) system of record for achieving full spectrum dominance. It is a suite of mission applications that provides critical joint warfighting C2 capabilities. GCCS-J is the principal foundation for dominant battle space awareness, providing an integrated, near-real-time picture of the battle space necessary to conduct joint and multinational operations. GCCS-J provides a robust and seamless C2 capability to the President, Secretary of Defense, National Military Command Center, combatant commanders, joint force commanders, and Service component commanders. It offers vital connectivity to systems the joint warfighter uses to plan, execute, and manage military operations.

2. GCCS-J Definition. Throughout this document, the term "GCCS-J" refers to GCCS-J SECRET, its strategic servers, and GCCS-T unless otherwise specified.

3. GCCS-J Classification. GCCS-J is a SECRET level system. GCCS-T is a TOP SECRET level system. GCCS-T will contain all safeguards to ensure TOP SECRET access follows DOD and National Security Agency (NSA) guidelines. GCCS-T provides the capability to transfer Focal Point information via Web, news, electronic mail, and file transfer protocol. GCCS-T will provide a public key encryption capability to ensure the privacy necessary for Focal Point control. CJCSM 3213.02A, "Joint Staff Focal Point Communications Procedures Manual," outlines specific procedures for Focal Point.

a. SECRET -- The unauthorized disclosure of this information or material could reasonably be expected to cause serious damage to national security.

b. TOP SECRET -- The unauthorized disclosure of this information or material could reasonably be expected to cause exceptionally grave damage to national security.

c. Releasability -- Access is restricted to personnel holding a final US SECRET clearance or final US TOP SECRET clearance for GCCS-T, and authorized under the National Disclosure Policy (NDP) and DODD 5230.11. Unless specifically annotated, CJCSI 5714.01 and several classification guides (i.e., CJCSM 3122.01 (JOPES), CJCSM 3122.03

(JOPES), and CJCSM 3150.02A (SORTS)) govern the releasability of GCCS-J software and information residing on GCCS-J.

d. All users having access to GCCS-J must possess a minimum of a final US SECRET security clearance as well as documented formal access approval, but not necessarily a need to know, for all data handled by GCCS-J. In the case of GCCS-T, all users having access must possess a minimum of a final US TOP SECRET security clearance as well as documented formal access approval, but not necessarily a need to know, for all data handled by GCCS-T. GCCS-J and GCCS-T must have a technical capability to control access to information based on a user's need to know.

4. Controlled Access Protection

a. System Access Control. Site personnel such as functional managers, system administrators, and security administrators must control, protect, and authorize access to GCCS-J.

b. Accountability. GCCS-J will provide individual user accountability including authentication, unique identification, and auditing.

c. Assurance. GCCS-J will incorporate a capability to protect internal data and programs from unauthorized access, tampering, or disclosure.

d. Documentation. GCCS-J and its strategic servers will each have a security features user's guide (SFUG) and a trusted facility manual (TFM) so the security environment of GCCS-J and the strategic servers can be appropriately established and maintained.

e. Discretionary Access Control. File owners will control, protect, and authorize access to GCCS-J files. The owner must verify the requester's need to know and clearance for the information.

ENCLOSURE B

GCCS MINIMUM SECURITY REQUIREMENTS

1. General Security Policy

a. All GCCS-J information is classified SECRET (or TOP SECRET in the case of GCCS-T) until determined otherwise and will be protected per DOD 5200.1-R. Safeguards will be applied to ensure that GCCS-J information and equipment is accessed only by authorized personnel, used only for its intended purpose, retains its content integrity, and is marked following DOD 5200.1-R.

b. Safeguarding of GCCS-J information and its resources (against sabotage, tampering, denial of service, espionage, fraud, misappropriation, misuse, or release to unauthorized persons) will be accomplished through the continuous use of safeguards consisting of administrative, procedural, physical and/or environmental, personnel, communications security, emanations security, and computer security (i.e., hardware, firmware, and software), as required. The mix of safeguards selected will achieve the requisite level of security or protection.

c. The safeguards selected for GCCS-J will ensure that the system meets the minimum requirements in DODD 8500.1 and DODI 8500.2. These minimum requirements will be met through automated and manual means in a cost-effective and integrated manner.

d. GCCS-J must meet the requirements established under National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11, "National Policy Governing the Acquisition of Information Assurance and IA Enabled Information Technology Products." A listing of approved products is available on the National Information Assurance Partnership homepage.

e. The interfacing and networking of GCCS-J with other Service and Defense agency information systems (ISs) are approved by the Joint Staff and controlled by the Service or Defense agency operating each IS. These connections must be supported by a memorandum of agreement (MOA) between the global GCCS-J DAA and the DAA of the interfacing or networking IS. Site GCCS-J DAAs may authorize the networking of local LANs and ISs with GCCS-J at the appropriate classification level and subject to the restrictions of this security policy. If there is a requirement for a locally approved connection, an MOA executed by the site GCCS-J DAA and the connecting network/IS DAA must support it. The Joint Staff must be notified of any MOAs executed by the site, and all MOAs must be in the site accreditation documentation. If the safeguards used in the two systems differ significantly, the site GCCS-J DAA may require re-accreditation. Networks supporting GCCS-T must not be connected to local LANs until approved devices are available to support this multiple security level requirement and the Joint Staff publishes a subsequent security policy.

f. All GCCS-J-related systems and program changes must comply with DOD and GCCS-J security policies. Changes include, but are not limited to:

(1) All applications and modifications.

(2) All common operating environment (COE) modifications that impact GCCS-J.

(3) All risks identified by the sites in accrediting GCCS-J locally.

g. DISA is the system engineer and integrator for GCCS-J and is responsible for ensuring that all applications and system components, including upgrades, comply with this policy. DISA and the Joint Staff must include early and continuous involvement with the site users, GCCS-J IAOs, data owners, and DAA(s) in defining and implementing security requirements of GCCS-J.

h. Mandatory statements of safeguard requirements will be included, as applicable, in the acquisition and procurement specifications for GCCS-J. The statements will be the result of a risk assessment and will, to the extent possible, identify the functional security requirement statements based upon the indicated level of trust required under DODD 8500.1.

i. The accreditation of GCCS-J will be a "type" accreditation from the Joint Staff/J-6 supported by a certification test and evaluation plan, threat assessment, a risk analysis of GCCS-J in its operational environment, an evaluation of the security safeguards, and a certification test and evaluation report, all approved by the global GCCS-J DAA. Each site, including combatant command, Service, or agency (C/S/A)-specific versions of GCCS-J, will take the "type" accreditation and apply local or C/S/A requirements (i.e., configuration, environmental impacts, etc.) to complete a local or C/S/A accreditation for approval by the GCCS-J site or C/S/A DAA. A separate "type" accreditation for GCCS-T is required.

j. The site or C/S/A GCCS-J DAA will ensure a program for conducting periodic reviews of the adequacy of the safeguards for the operational and accredited GCCS-J is established. To the extent possible, reviews should include persons who are independent of the user organization and the GCCS-J operation or facility.

k. All major changes to type-accredited GCCS-J must be reviewed for certification by DIA and re-accredited by the Joint Staff/J-6 as necessary prior to implementation at sites. A major change shall be defined as any change to system functionality, components, or code that have the potential to materially change the security posture of GCCS-J. The global GCCS-J DAA will determine whether a given change will be categorized as major. Minor updates to system functionality or the application of security fixes are not to be categorized as major.

l. Procedures are to be established and documented by a configuration management (CM) plan to ensure that CM is done in a specified manner following the GCCS-J configuration management policy in CJCSI 6722.01A. CM ensures changes take place in an identifiable and controlled environment and do not adversely affect any properties of the system. It provides assurance that additions, deletions, or changes made to the system do not compromise the trust of the originally evaluated system. CJCSI 6722.01A defines how the Joint Staff approves applications, data, and equipment for use and how they are introduced into GCCS-J for use by the sites. Sites are permitted to install software outside the standard GCCS-J configuration. The instruction explains how sites should identify non-standard software to the Joint Staff. That software will require local security certification to the level of GCCS-J. Non-GCCS-J approved software implemented at a site must be included in the site certification and accreditation documentation. GCCS-T changes will only be approved by the Configuration Management Board (CMB) and accredited by the Joint Staff/J-6.

m. Each GCCS site will establish a program for developing and testing contingency plans and recovery procedures. The objective of contingency planning is to provide reasonable continuity of GCCS-J support if events occur preventing normal operations. Plans should be tested periodically under realistic operational conditions.

n. All GCCS-J users will possess a minimum of a final US SECRET clearance or, in the case of GCCS-T, a minimum of a final US TOP SECRET clearance. GCCS-J will be operated following the NDP. Anyone requesting a waiver to the NDP must submit it to the Joint Staff/J-3 for approval. The Joint Staff/J-3 will forward it to the Joint Staff/J-6 for review and approval. Data access is approved or granted by local functional managers and restricted to incidental access only. Contractors must be monitored and activities controlled through appropriate tasking from US government (USG) employees, sufficient government oversight as defined and provided by the site, and review of contractor deliverable products.

o. The site GCCS-J IAO is responsible for ensuring proper safeguards are in effect to restrict access to GCCS-J. The site GCCS-J IAO will control all access mechanisms.

p. The site GCCS-J IAO must report all security incidents, as determined by the site GCCS-J DAA, to the regional and C/S/A computer emergency response team (CERT), Joint Task Force – Global Network Operations (JTF-GNO), and the Joint Staff/J-6.

q. All enclaves running GCCS-J or GCCS-T should be hosted on a network that uses a technology that minimizes an attacker's opportunity to sniff network traffic and provides additional defense-in-depth.

r. Host machines on GCCS-J shall not use standard names indicative of the host's function. Assigning descriptive names to host machines can give a malicious user valuable information as to the machine's function (i.e., pop3.GCCSsite.smil.mil is a POP3 mail server) and can aid in developing an attack in the system.

s. Anti-virus software shall be loaded on each GCCS-J workstation and server prior to operational use. Updated anti-virus scan software will be provided periodically by DISA. Any diskette and/or media introduced into a GCCS-J workstation shall first be tested for malicious code. Any writeable, removable media (to include floppy disks, backup tapes, zip disks, and writeable compact discs (USB-based storage devices known as thumb or flash drives are strictly prohibited on GCCS-J)) introduced into a GCCS-J workstation shall be labeled as required by established policies and the local site security standard operation procedures (SOPs).

t. Additional guidance for GCCS-T:

(1) GCCS-T is a closed network used for processing of TOP SECRET information.

(2) The SECRET Internate Protocol Router Network (SIPRNET) is the transport mechanism for GCCS-T. GCCS-T data is cryptographically

isolated from the SIPRNET using approved TYPE-1 encryption devices. Sites must be connected to their server sites through an approved TYPE-1 encryption device.

(3) DISA/Joint Staff Support Center, NSA, and Joint Staff/J-6X will manage all configuration changes to the bulk encryption devices for GCCS-T.

(4) Since GCCS-T is operated as a closed system, sites are prohibited from connecting any other LAN or separate system to GCCS-T without first obtaining written approval from Joint Staff/J-6.

(5) To tightly control expansion of GCCS-T, all requests for new GCCS-T workstations and servers shall be submitted to the Joint Staff/J-3 Deputy Directorate for Global Operations, Command Systems Operations Directorate (DDGO/CSOD) for validation, copy to Joint Staff/J-6 and the GCCS-J Program Management Office (DISA).

(6) The processing of special handling data on GCCS-T such as Secure Identification Operating Procedure (SIOP) and Special Category (SPECAT) is prohibited under the current type accreditation.

(7) Periods processing on any piece of GCCS-T equipment (workstations, servers, and network encryption system devices) is prohibited.

(8) Limit site-unique software to that which is provided through authorized CM procedures. Before loading any software on GCCS-T other than that authorized under the currently approved version description document or security patch release, sites will coordinate with the GSO to ensure:

(a) J-3/DDGO/CSOD validates operational requirement.

(b) DISA validates proper installation packaging of the software.

(c) Sites conduct verification testing to ensure that the software will not negatively impact the configuration or the security posture.

(9) Physical security of installed components is dependent on local security policies and procedures IAW this policy.

u. GCCS minimum-security requirements will be met through automated or manual means in a cost-effective manner and integrated fashion.

2. General Security Requirements

a. Mission Assurance Category and Level of Confidentiality. The mission assurance category for GCCS-J is Mission Assurance Category I, Classified. This reflects the information handled by the system relative to requirements for integrity (including authentication and non-repudiation) and availability services. Joint Staff/J-6 assigned the mission assurance category based on criteria provided in DODI 8500.2.

b. System Library Management Controls. System libraries shall be managed and maintained to protect privileged programs and to prevent or minimize the introduction of unauthorized code.

c. System State Changes. System initialization, shutdown, and aborts shall be configured to ensure the system remains in a secure state. In addition, tests shall be periodically run to ensure the integrity of the system state.

d. Waivers. Any site waiver to GCCS-J security requirements, service oriented architecture, or COE requirements that support GCCS-J security must be submitted to the GCCS-J GSO for either approval or notification. Sufficient documentation must accompany all waiver requests and be included in the site certification and accreditation documentation. This is not an automatic process and enough time shall be allowed so if the waiver is not approved, the Program Manager will have ample time to implement an alternate solution. Waiver authority can be found in Enclosure E, "GCCS Security Policy Waiver Authority."

e. Mobile Code. The GCCS-J security policy for mobile code implementations provides detailed guidance on the implementation of mobile code in the GCCS-J environment.

f. Re-accreditation Assessment. The site GCCS-J DAA's designated representative to the local CMB shall notify the site GCCS-J DAA of requests for deviations to the GCCS-J baseline configuration that impact security, and a re-accreditation determination must be made by the site GCCS-J DAA. If the request for change is approved, the site GCCS-J DAA shall inform the global GCCS-J DAA if the change impacts security.

g. Metrics. Service level agreements, or equivalent, shall be established between the using organizations and computing service providers. When functional availability requirements exist, they shall be described in specific operational and service-level agreements.

h. Portable Devices. Except as specifically provided in waivers from the global GCCS-J DAA, GCCS-J software and data shall not be transferred to portable devices (excluding laptops). Additional guidance on portable devices can be found in Enclosure G, "GCCS-J Policy Memorandum, Personal Digital Assistants/Personal Electronic Devices (PDA/PED) Policy." Periods processing and wireless capability are prohibited on laptops that have GCCS-J software loaded and access GCCS-J data.

i. Keyboard, Video, Mouse (KVM) Switches. Use of NSA/Central Security Service (CSS) and/or Defense Information Systems Network Security Accreditation Working Group (DSAWG)-approved KVM switches is authorized on GCCS-J with site GCCS-J DAA approval. For additional guidance, see Enclosure H, "GCCS-J Keyboard, Video, Mouse (KVM) Switch Policy."

j. Web Servers. Any Web server software used by GCCS-J sites will reside on its own physical device, separated from and independent of other GCCS-J servers. Web server software is defined as any software or system that provides Web content to users or systems outside of the enclave or DMZ where the Web server is located. A server providing a web portal to users outside the enclave would be considered a Web server. A server providing application services for servers within the same enclave, even if it uses HTTP(s) as its transport, is not considered a Web server.

k. Software. GCCS-J users are prohibited from loading software on GCCS-J workstations and servers without approval from the site GCCS-J DAA, who in turn informs the global GCCS-J DAA. Software using the simple network management protocol (SNMP) is not sanctioned for use on GCCS-J or GCCS-T unless authorized by the Joint Staff/J-6X. Applications using SNMP must implement "community strings" that follow the same guidance found in the GCCS-J TFM for developing strong passwords.

l. Wireless Technology. The use of wireless technology is prohibited on GCCS-J unless authorized by the global GCCS-J DAA.

3. Acquisition

a. Security in IT Services. Acquisition or outsourcing of IT services shall explicitly address government, service provider, and end user security roles and responsibilities.

b. Dedicated Security Services. Acquisition or outsourcing of dedicated security services such as incident monitoring, analysis, and response; operation of IA devices such as firewalls; or key management services shall be coordinated by the responsible DAA.

c. Architecture and Design Standards

(1) Compliance with the international common criteria (CC) shall be used to establish security design and architectural parameters for acquisition initiatives. Priority shall be given to compliance with DOD and then US federal government protection profiles. If CC-evaluated products are not available, then prevailing "best departmental practices" such as those outlined in the information assurance technical framework or the DOD Information Technology Standards Registry shall be used to establish security design and architectural parameters for acquisition initiatives. When CC-evaluated products are not available, then a custom or tailored standard developed or approved by a respected entity, such as NSA, is used to establish security design and architectural parameters for acquisition initiatives. Also, communications security (COMSEC) acquisitions shall comply with DODD C-5200.5.

(2) GCCS-J and strategic server TFMs with instructions for the minimum expected configuration shall be provided. These shall be instructions for field implementation and shall apply to GCCS-J servers and user workstations accessing these servers.

d. Commerical and Government Off-the-Shelf (COTS/GOTS) Procurement Practices. Any product used on GCCS-J should be installed and configured so as not to degrade the security of the workstation, server, or network on which the product is installed. The Department of Defense has a requirement to use COTS products whenever practical.

e. Identification and Authentication (I&A), Digital Signature, and Encryption Standards. GCCS-J will migrate to public key infrastructure (PKI) following DOD guidance.

f. Configuration Specifications. Security configuration or implementation guidance for the deployment of newly acquired IT assets shall be developed via a custom test and review process conducted by a respected entity such as DIA that is independent of the developer, integrator, or sponsor for the acquisition.

4. Change Control

a. Software Change Controls. Change controls for software shall be in place to prevent unauthorized programs or modifications to programs from being implemented.

b. Production Change Controls. GCCS-J and strategic server operation shall be specified in the TFMs and operated as specified. Exceptions shall be shown in the signed field and/or site accreditation documents.

c. Program Implementation. An effective application control program shall be implemented and will include: instructions for restart and recovery procedures; restrictions on source code access, system utility access, and system documentation; protection from deletion of system and application files; and a structured process for implementation of directed solutions, e.g., information assurance vulnerability alert (IAVA). In addition, audit or other technical measures shall be in place to ensure the application controls are not compromised and application change controls are periodically tested.

5. Continuity of Operations

a. Identification of Critical Functions. GCCS-J sites will identify all assets supporting critical functions (i.e., computer-based services, data and applications, and physical infrastructure).

b. Disaster and Recovery. GCCS-J sites shall have a disaster plan that provides for the smooth transfer of all operations to an alternate site for the duration of an event with little or no loss of operational continuity. (Disaster recovery procedures include business recovery plans, system contingency plans, facility disaster recovery plans, and plan acceptance.)

c. Contingency Planning. GCCS-J sites will develop and test contingency plans following Office of Management and Budget (OMB) Circular No. A-130 to ensure GCCS-J security controls function reliably and adequate backup functions are in place so continuous security functions are maintained during interrupted service. Procedures must be in place to recover data if modified or changed. Contingency plans will be documented in the site's accreditation documentation and shall include disaster recovery guidance.

d. Alternate Site Designation. GCCS-J sites will have an alternate site that permits the resumption of critical functions.

e. Secure Recovery. GCCS-J sites will implement recovery procedures and technical system features to ensure recovery is done in a secure and verifiable manner. Circumstances that can cause a non-secure recovery shall be documented and appropriate mitigating procedures shall be put in place.

f. Scheduled Exercises and Drills. The Disaster Recovery Plan or significant portions thereof shall be exercised semi-annually by GCCS-J sites.

g. Enclave Boundary Defense. GCCS-J subnet boundary defense at the alternate site shall provide the same levels of defense as the primary site. In addition, GCCS-J subnet boundary defense at the alternate site shall be configured identically to the primary site.

h. Data Backup Procedures. Data backup shall be accomplished by maintaining a redundant secondary system, not collocated, that can be activated without significant loss of data or disruption to the operation.

i. Maintenance Support. Maintenance support shall be available to respond 24/7 immediately upon failure of critical components.

6. Critical Utilities and Supplies

a. Backup Copies of Critical Software. Backup copies of the operating system and other critical software shall be stored in a fire rated container that is not collocated with the operational software.

b. Defense in Depth Architecture. GCCS-J shall follow an enterprise-wide IA architectural overlay consistent with the overall Global Information Grid (GIG) Architecture, and implement a defense-in-depth strategy to establish and maintain an overall acceptable IA posture across the GIG.

c. Long-Haul Communications Services. Arrangements for alternate long-haul communications services capable of restoring full operations without loss of operational continuity shall be in place.

d. Power Supply. An uninterrupted power supply shall be installed on all GCCS-J devices, or an alternate power supply source capable of continuing full operations shall be provided.

e. Spares and Parts. Maintenance spares and spare parts shall be available 24/7 immediately upon failure of critical components.

7. Asset Management

a. Hardware Baseline. A current and comprehensive baseline inventory of all hardware required to support GCCS-J operations shall be maintained by the field, and a backup copy of the inventory shall be stored in a fire-rated container or otherwise not collocated with the original.

b. Software Baseline. A current and comprehensive baseline inventory of all applications and software required to support enclave operations shall be maintained by the responsible configuration control board, and a backup copy of the inventory shall be retained but must not be collocated with the original. Each management level shall maintain inventory unique or modified for their level.

c. Apply Patches. GCCS-J will encompass all current and appropriate security and virus patches approved for all GCCS-J baseline software packages within each current release.

d. Vulnerability Management. A comprehensive vulnerability management process compliant with CJCSI 6510.01D shall be implemented at all levels of GCCS-J. The process shall include periodic vulnerability assessments and a formal review every 12 months. The process will apply to the joint level combatant commander and/or Service implementations and sites as appropriate. A risk management program will be implemented by both the global GCCS-J DAA and site GCCS-J DAAs to determine how much protection is required, how much exists, and the most economical way of providing needed protection.

e. Life Cycle Management (LCM). Procedures shall be in place to provide end-to-end management of security functions and features over the lifecycle of GCCS-J.

f. Quality Assurance. A quality assurance program modeled after ISO 9000 or other prevailing quality standard (e.g., commercial best practices) shall be implemented that incorporates IA requirements for all GCCS-J.

g. Security Enterprise Management. The key to successful security management in a distributed environment is to have tools that support managing by exception. The complexity of managing security in a distributed environment along with the staff limitations require that GCCS-J automate more of the security administrative functions. Tools shall be provided for the security staff to assist in security enterprise management. Performance management data will be gathered using smart agents resident on various hardware platforms or LAN segments. These segments will set up automatic fault reporting back to the GCCS Management Center (GMC) Pentagon. Performance management agents may also be configured with the IP address and/or DNS names of the site's or organization's management stations so they can also receive the performance management data.

h. Software Security Design. The software security design shall incorporate best security practices and the common criteria.

i. Trusted Facility Manual. All GCCS-J sites shall be consistent with the GCCS-J TFM. Exceptions and deviations are to be identified in accreditation documents provided to Joint Staff/J-6X.

j. Boundary Defense. GCCS-J shall be isolated at each site from the surrounding non-GCCS-J infrastructure by operating the GCCS-J servers on an isolated subnet. All GCCS-J servers will be located in this enclave. It is recommended that GCCS-J clients are also located in the GCCS-J enclave. At a minimum, GCCS-J clients must be located in the local site, post, and/or station enclave. Sites should follow guidance provided in the GCCS-J Filter Router Access Control Lists document.

k. Connection Rules. GCCS-J shall be compliant with pertinent DOD connection rules and approval processes.

l. Virus Protection. All servers, workstations, and mobile computing devices shall implement the local C/S/A virus protection scheme.

m. Intrusion Detection System (IDS). GCCS-J shall be monitored to detect, isolate, and react to intrusions, disruption of services, or other incidents that threaten the security of DOD operations or IT resources, including internal misuse. An IDS plays a vital role in maintaining the security of any computer system and can be deployed as part of the "Defense In Depth" strategy. The lack of such capability could allow known malicious activity to go unnoticed until after the fact.

n. Security Rules of Behavior. A set of rules describing the security operations of GCCS-J and clearly delineating security responsibilities and expected behavior of all personnel shall be in place. The rules must include the consequences of inconsistent behavior or non-compliance. Signed acknowledgement of the rules shall be a condition of access.

o. Network, System, or Application Integrity Analysis Tools. Only properly segmented, tested, configured, and Global DAA-accredited tools for automatically monitoring the integrity of GCCS-J and GCCS-J enclaves and the GCCS-J applications shall be deployed.

p. Enforcing Policies Between Enclaves. GCCS-J shall use some automated means of enforcing policies between enclaves.

8. Security Documentation

a. Development Documentation. Documentation shall include, at a minimum, security-specific documentation for installation and operation of the system (TFM), administration of the system, and use of the system (SFUG). Some applications may require a separate SFUG (e.g., JFRG) where the information does not need to be available to all users in the GCCS-J SFUG.

b. Accreditation Documentation. Accreditation documentation in compliance with current DOD C&A guidance and regulations shall be established.

9. Logical Access

a. Interconnection. Differing need to know requirements between interconnecting DOD systems or GCCS-J subnets shall be handled by discretionary access controls.

b. Key Management. Symmetric keys shall be produced, controlled, and distributed using NSA-approved key management technology and processes. Asymmetric keys shall be produced, controlled, and distributed using DOD PKI Class 4 certificates and/or hardware security tokens that protect the user's private key.

c. Policy or Role Based Access. User access to GCCS-J shall be accomplished through a policy- or role-based access scheme that establishes methods to ensure appropriate users can create, modify, and review information and transactions for which they are responsible. and/or have a need to know.

d. Marking and Labeling. GCCS-J shall follow all requirements for marking and labeling contained in policy and guidance documents such as DOD 5200.1-R. Markings and labels shall clearly reflect the classification level, if applicable, and any special dissemination, handling, or distribution instructions.

e. Marking. GCCS-J output shall be marked to reflect the accurate sensitivity of the information. Requirements for security classification and applicable markings for classified information are in DOD 5200.1-R. Markings may be automated or performed manually. Accuracy of automated markings on output must not be relied on, unless the security features and assurances of the IS meet the minimum requirements as specified in DODD 8500.1 and DODI 8500.2. If the requirements are not met, but automated controls are used, all output shall be protected at the SECRET level (or TOP SECRET for GCCS-T) until manually reviewed by an authorized person to ensure the output was marked with the proper classification and caveats. All media and containers will be marked and protected at the SECRET level (or TOP SECRET for GCCS-T) until the media are declassified, degaussed, or overwritten using a DOD-approved methodology, following DOD 5220.22-M, "National Industrial Security Program Operating Manual," or unless the information is declassified or downgraded following DOD 5200.1-R.

f. Communications Security. COMSEC shall support accountability of users, least privilege, and integrity by providing confidentiality of communications and non-repudiation of users.

(1) Accountability. Safeguards will be in place to ensure persons having access to GCCS-J will be held accountable for their actions. An audit trail will provide a documented history of GCCS-J use. The audit trail will contain sufficient detail to reconstruct events when determining if a compromise has taken place and if so, the severity and extent of the compromise. Audit records will be retained for 2 years or longer as directed by Service or combatant command requirements; to fulfill this requirement, the manual and/or automated audit trail will document:

(a) The identity of each person and device with access to GCCS-J. Each authorized GCCS-J user and resource will have a unique system identity such as a user account (userid). Users will be required to identify (via individual user accounts) and authenticate themselves (i.e., passwords) prior to accessing system resources. The use of unauthorized group accounts is prohibited.

(b) The time of access and egress. Each individual user log-on and log-off will be audited.

(c) Specific user activity. These activities will be sufficient to ensure user actions are controlled and open to scrutiny (audit flags to be used as a minimum are specified in the TFM). The audit events, as a minimum, will include log-in/log-out, selected administrative actions or changes in security events, failed deletion events, and failed read/write. Each site may include additional events as dictated by mission requirements.

(d) Activities that might modify, bypass, or negate safeguards controlled by the system.

(2) TEMPEST. GCCS-J does not normally require TEMPEST configurations. However, if the JTF commander or combatant commander determines TEMPEST is required, the GSO must be notified.

g. Account Control. A comprehensive account management process shall be implemented to ensure only authorized users can gain access to workstations, applications, and networks and that individual accounts designated as inactive, suspended, or terminated are promptly deactivated or removed.

h. User Identification. Access to GCCS-J shall be granted to individuals based on need to know and following DOD Regulation 5200.2-R for clearance, special access, and automated data processing category designation requirements and qualifications. Site GCCS-J DAAs shall follow GCCS-J user management requirements as specified in the TFM by establishing a local user management process to assign users a GCCS-J identifier and associate the appropriate roles to that user. GCCS-J shall support user management by providing roles that can perform these actions locally. This includes assigning GCCS-J user identifiers, associating roles within their authority to those user identifiers, and changing passwords per their local process.

i. Individual Identification and Authentication. GCCS-J access is gained through individual identifiers such as a unique user ID and password.

j. Group Accounts. The following administrative group accounts within GCCS-J were designed to divide the absolute power of the root user: KEYMAN, SA, SYSADMIN, SECMAN, and JOPESDBA. These accounts are a security mitigation to limit the number of administrators requiring access to root. These administrative group accounts enable the establishment of multiple, special purpose system administrators and thereby enforce the concept of least privilege, especially when used for tasks not requiring full root privilege. The global GCCS-J DAA authorizes the use of these accounts in conjunction with the following procedures:

(1) GCCS-J sites will limit administrative group account access to authorized system administrators.

(2) In order to ensure auditing capability, direct log-in to an administrative group account is strictly prohibited.

(3) In order to access the accounts identified in paragraph j above, authorized users must first log in using their individual user id and password and then super-user (su) to the appropriate account.

k. System Accounts. System accounts are characterized by their use to pass information between two existing applications or databases on an ongoing basis. Data may be passed uni-directionally or bi-directionally, i.e., read-only or read and write-back. Individual users are prohibited from using system accounts to gain access to data. Therefore, system accounts will not disclose or disseminate data beyond the linked systems. The use of authorized system accounts may reduce loads on GCCS-J databases by moving redundant data requests to servers local to the end user, and/or reduce data access waits for end users by allowing data forwarding, storage, and/or fusing prior to data calls.

(1) An example of an authorized system using a system account would be as follows: the external interface system presents data to the end users in a unique manner, not supported by GCCS-J. The external interface system audits users, log-ons, and data access and maintains records of the information. The external interface system maintains a copy of the access permissions data gained from the originating system(s) and limits the user's access to the same or less as would be gained by accessing the GCCS-J system directly.

(2) Any GCCS site or external interface that uses a system account to access GCCS-J data must request approval from the Joint Staff/J-6 to authorize use of the account. The request should be submitted in writing to the Joint Staff/J-6 and provide identification of the system account required, a justification for use of the account, a description of how the account is implemented, an explanation of control and auditing procedures, and local points-of-contact. The Joint Staff/J-6 will provide a coordinated (DIA, DISA, Joint Staff/J-3) response to the requesting organization. Once approved, the system account will be included in a MOA between GCCS-J and the GCCS site or external interface.

(3) MOAs must describe how the external interface identifies individual users and audits access to GCCS-J (GSORTS, JOPES CLASSIC, and/or JOPES 21) data. The MOA must provide points of contact, guidelines for how the system account is implemented, and individual accountability and audit procedures pertaining to the external interface accessing GCCS-J (GSORTS, JOPES CLASSIC, and/or JOPES 21) data. User and audit information must be maintained in accordance with this security policy and provided upon request from the GCCS-J Program Management Office or the global GCCS-J DAA. External interfaces approved to use system accounts must also adhere to all guidance in this security policy.

(4) System accounts will only be authorized to pass data between two applications and/or databases. No system account will be used to access data for a user. These accounts are not considered group accounts as no individual or group of users will be able to access data with these accounts. The receiving system and its owning C/S/A

assume full responsibility for the required levels of control, protection, and access limitations on any data originating from a GCCS-J system or database. If there is a violation of this policy, the GMC has the authority to disconnect the interface to protect GCCS-J data and resources.

(5) All external interfaces connecting to GCCS-J applications and/or databases must ensure all users have appropriate access rights and clearances prior to allowing access.

l. Authentication by Password. GCCS-J shall provide password authentication of users. Authentication verifies who the user claims to be. As such, the authentication mechanism must be trusted. Passwords shall be protected through encryption while on any portion of the network and not pass through any part of the network in the clear. Non-repudiation of the authentication shall be supported by the strengths of the password mechanism.

m. Strong Authentication for Web Connections. GCCS-J, in compliance with standard DOD policy, shall provide strong authentication for Web connections. Non-repudiation of the authentication shall be supported by the strengths of the password mechanism. Specifically, PKI certificates shall be used to support confidentiality, authentication, and non-repudiation. Public key certificates in GCCS-J shall follow the DOD PKI policy and associated guidance.

n. Non-Repudiation. Non-repudiation shall be provided to ensure individuals, identified by their user identifier, are held accountable and cannot deny their actions. GCCS-J shall provide identification, authentication, and audit in support of non-repudiation of accountability. GCCS-J shall identify who the user is through identification, verify whom the user claims to be through authentication, control access through the identification information correlated to the role(s) the user is assigned, and track security-related actions using this identification. The mechanisms performing these functions shall be robust enough to ensure non-repudiation and provide a sufficient trail of evidence for any legal actions required as a result of activities a user performed. In order to support the transition to a network-centric environment, the global GCCS-J DAA may approve trust relationships with other DOD authentication sources such that GCCS-J will trust users authenticated by approved external systems. GCCS-J will maintain individual identity and audit trail requirements for externally authenticated users.

o. User Account Removal and Review. Procedures shall be established to ensure that, upon specific personnel actions, the user's accounts will be immediately disabled. At a minimum, these actions include extended leave, furlough, firing, transfer, or retirement. Before deleting their accounts, privileges, and data files, account managers shall review the individual's computer access and reassign information assets to replacement(s) as necessary. In addition, the individual's supervisor shall ensure each user's access is appropriate and limited to the privileges necessary for their job and shall review the privileges associated with each user account annually.

p. Remote Access Review and Reconciliation. Procedures shall be established to ensure remote database access accounts are validated semi-annually by all GCCS-J sites.

q. Root Access. GCCS-J sites will limit access and use of root log-in capability to system administrators only. In addition, GCCS-J sites will maintain accountability of each occurrence when root log-in is used. The site GCCS-J DAA must authorize the use of root log-in capability in writing and ensure that the password is only provided to approved system administrators. In order to log-in as root, authorized administrators must first log-in using their individual user id and password and then super-user (su) to root. Direct log-in to root should only be used in emergency situations and during builds. If direct root log-in is required, except during builds, the authorized user must record this direct access (name, date, time of direct root log-in, time of direct root log-out) in a log book.

10. Physical Access

a. Access. An access control procedure will be in place for each GCCS-J site. It will include features and/or procedures to enforce the access control policy of the information within GCCS-J. The identity of each user requesting access to GCCS-J will be positively established before authorizing access.

b. Data Interception. Devices that provide output or display information in human-readable form shall be positioned to deter unauthorized individuals from reading the information.

c. Physical Controls. GCCS-J hardware, integrated operating system software, design documentation, and all its data will be protected to prevent unauthorized (intentional or unintentional) disclosure, destruction, or modification. Data integrity shall be maintained. The level of control and protection will be commensurate with the guidelines for SECRET or TOP SECRET information for GCCS-T, to include personnel, physical, administrative, and configuration controls. Additionally, protection against denial of service of GCCS-J resources (e.g., hardware, software, firmware, and information) shall be consistent with the sensitivity of the information handled by the IS.

(1) DOD executive agents of GCCS-J software applications will use adequate means of physical controls at the sensitive but unclassified level in the respective developmental activity.

(2) GCCS-J software, hardware, firmware, and data, once installed, are classified SECRET (TOP SECRET in the case of GCCS-T). Both must be protected following the requirements set forth in DOD 5200.1-R. Protecting access to the SIPRNET must be controlled and protected to ensure continued integrity of the network is maintained. Implementation of physical controls to protect this information may depend on GCCS-J workstation configuration. For TOP SECRET information, the only alternative implementation solutions are defined in DOD 5200.1-R, Chapter 6. However, with SECRET information DOD 5200.1-R permits additional solution capabilities through technology in implementing GCCS-J SECRET workstations. Configurations of these workstations will include either a non-removable or a removable hard drive. IAOs must be fully aware of this policy to properly manage their respective areas. Minimum physical security requirements are:

(a) Unauthorized personnel must not be able to view information on the GCCS-J workstation screen of an authorized GCCS-J user.

(b) For protection of TOP SECRET information in a secure room, an alarm system must be installed following Appendix G, DOD 5200.1-R. This is required for all workstations accessing GCCS-T regardless of whether removable hard drives are available.

(c) GCCS-J workstations with non-removable hard drives and not under the personal control of an authorized user 24/7 shall be guarded or stored in a locked security container, vault, room, or area as outlined in DOD 5200.1-R, Chapter 6 and Appendix G. If an approved security container, vault, room, or area is not available, then the GCCS-J SECRET workstation protection may be implemented in the following manner:

1. A cleared guard or duty personnel must provide continuous protection.

2. The cleared guard or duty personnel must inspect the area where the workstation is installed or an alarm system must be installed with appropriately cleared personnel responding to any alarm within 30 minutes (15 minutes for TOP SECRET).

3. The workstation with a non-removable hard drive must be under the control of an authorized user 24/7.

(d) GCCS-J workstations with removable hard drives and portable computing devices (i.e., laptops) may be implemented as described above or if necessary -- although not recommended -- in less secure rooms or areas subject to the following stipulations:

1. IAOs must continually monitor such installations and ensure access procedures are in local SOPs and operating instructions.

2. Store workstations in a room providing protections against denial of service, destruction, and modification of the equipment as implemented through local security SOPs and approved by the site GCCS-J DAA.

3. Never leave the GCCS-J workstations unattended with the hard drives or SIPRNET connection not secured.

4. Store removable hard drives and portable computing devices in a GSA-approved container for SECRET information when not in use. This container will be in a secure area.

5. Secure the SIPRNET connections with a locking mechanism having an adequate data encryption device.

6. The position of the GCCS-J workstation screen must ensure information cannot be viewed by casual observation or unauthorized personnel when in use by the authorized GCCS-J user.

7. Site GCCS-J DAA and IAO will ensure procedures are in place and users are trained to observe this policy.

8. Report violations to the IAO. The IAO will report these violations in a quarterly report to the GSO. Immediately report any severe violations to the GSO or the GMC/Network Operations Center (GMC/NOC).

(e) All other GCCS-J equipment must be installed in a GSA approved vault, room, container, or area. Due to the critical nature of GCCS-J servers, they must be accessible only through controlled means within the secure room, vault, container, or area. Examples are: locked in a secure closet in a secure room; locked in a cable or telephone closet in a secure room; or in a locked cabinet in a secure room. Adequate environmental controls (air and humidity) must be maintained. The importance of restricting physical access to any GCCS-J server cannot be overemphasized.

(f) In field and combat operations, this policy of accountability, dissemination, transmission, and storage of classified information and material may be modified by military commanders who are responsible for ensuring adequate security is maintained for GCCS-J. Modifications to this policy for use in planned field and combat operations will be forwarded to the GSO for review prior to operation commencement. Unplanned field and combat operations use of GCCS-J will be reviewed in an after-action report.

d. Internal Security Procedures. Procedures to ensure the proper handling and storage of information shall be implemented, such as end of the day security checks and unannounced security checks.

e. Physical Access to Workstations. Only personnel with an acceptable need to know and appropriate clearances shall be granted physical access to workstations or facilities displaying, storing, or processing sensitive or classified information or information requiring special handling or limited distribution.

f. Visitor Control. Current signed procedures shall exist for controlling visitor access and maintaining a detailed log of all visitors to the computing facility.

g. Physical Access to Computing. Every physical access point to facilities housing IT assets critical to local GCCS-J operations (i.e., computing facilities) shall be guarded or alarmed 24/7. Two (2) forms of identification shall be required to gain access to the facility (e.g., photo and key card). Internal access restrictions are not required. In addition, all access points shall be observed 24/7, and intrusion alarms shall be centrally monitored. Internal access shall be restricted based on need to know and enforced by a third form of identification (e.g., password, cipher lock combination).

h. Physical Access Control for Workstations. Physical access controls shall be provided for GCCS-J workstations.

i. Storage. Store documents and equipment in approved containers or facilities with maintenance and accountability procedures following DOD 5200.1-R.

j. Labeling. GCCS-J output shall be marked to reflect the accurate sensitivity of the information. Requirements for security classification and applicable markings for classified information are in DOD 5200.1-R.

Markings may be automated or performed manually. All output shall be protected at the SECRET level (or TOP SECRET for GCCS-T) until manually reviewed by an authorized person to ensure the output was marked with the proper classification and caveats. Mark and protect all media and containers at the SECRET level (or TOP SECRET for GCCS-T) until the media are declassified, degaussed, or overwritten using a DOD-approved methodology, following DOD 5220.22-M, "National Industrial Security Program Operating Manual," or unless the information is declassified or downgraded following DOD 5200.1-R.

k. Clearing and Sanitizing. All documents, equipment, and machine-readable media containing sensitive or classified data shall be cleared and sanitized before reuse within the Department of Defense. These items will not be released outside of the Department.

l. Destruction. All documents, machine-readable media, and equipment shall be destroyed using procedures that comply with DOD policy, e.g., DOD 5200.1-R.

m. Secure Disposal. At each site, ensure individuals are trained in responsibilities for the disposal of all sensitive and classified GCCS-J hardcopy products; clearing and securing all GCCS-J media; and clearing and securing disposal of all GCCS-J hardware identified for reassignment or disposal.

11. Data Integrity

a. Encryption for Data Integrity. Implementation of specific non-repudiation capabilities such as digital signatures shall exist.

b. Data Integrity. Safeguards will be in place to detect and prevent inadvertent or malicious modification or destruction of data. Each file or data collection in GCCS-J shall have an identifiable source throughout its life cycle. Accessibility, maintenance, movement, and disposition shall be governed by security clearance, formal access approval, and need to know.

c. Changes to Data. Access control mechanisms shall exist to ensure data is accessed and changed only by authorized personnel. In addition, access and changes to the data shall be recorded in transaction logs that are reviewed periodically or immediately upon system security events. Users shall also be notified of time and date of the last change in data content.

12. Personnel Security

a. Need To Know. Access to any information requiring special protection measures or restricted distribution, such as classified or official information, or to unclassified information not approved for public release, shall be based on a strict need to know as determined by the data owner and demonstrated by assigned official government duties.

b. Least Privilege. In addition to the appropriate security clearance level and need to know authorization, access procedures shall enforce the principles of separation of duties and least privilege. GCCS-J shall function so each user has access to only entitled information by virtue of clearance and formal access approval. In the case of need to know for GCCS-J information, access must be essential for accomplishment of lawful and authorized government purposes.

c. Access to Classified Information. Individuals requiring access to official or classified information shall be processed for access authorization following DOD personnel security policies. GCCS-J and its strategic servers operate on a high level of confidentiality. Individuals accessing systems operating on a high confidentiality level shall be cleared to the highest level of classification processed on that system. The operating environment of GCCS-J and its strategic servers must also have the appropriate internal and external system exposure for its high level of confidentiality.

d. Security Clearance. A DOD-approved security clearance at a minimum of final US SECRET is required for access to GCCS-J environment or system. Each site must have a process in place to verify security clearances through the proper authority prior to allowing access to GCCS-J environments or systems. A final US TOP SECRET is the minimum acceptable for access to GCCS-T.

e. Training. A program shall be implemented to ensure that, upon arrival and periodically thereafter, all personnel receive training and familiarization to perform their assigned IA responsibilities, to include familiarization with their prescribed roles in all IA-related plans such as incident response, configuration management, and continuity of operations or disaster recovery. Role-specific security training shall be provided to each developer, integrator, certifier, accreditor, security official, and manager that makes decisions with security impact on GCCS-J. Each GCCS-J site will have a GCCS-J education, training, and awareness program covering the security needs of all persons accessing GCCS-J servers and clients. The program will ensure that persons responsible for GCCS-J and its information are aware of proper operational and security-related procedures and risks. Security awareness of GCCS-J should be incorporated into each site's annual security awareness program. GCCS-J Training Management (CJCSI 6721.01A) defines the role of the Single Service Training Manager (SSTM). The SSTM Web sites provide information on GCCS-J Security and Security Administrator courses.

f. User Certification. GCCS-J roles that require advanced training beyond standard user roles shall be defined and have an associated certification program.

g. Maintenance Personnel. Only authorized personnel shall perform maintenance. The processes for determining authorization and the list of authorized maintenance personnel shall be documented. In addition, except as authorized by the DAA, personnel who perform maintenance on classified ISs shall be cleared to the highest level of information on the IS. Cleared personnel who perform maintenance on a classified IS require an escort unless they have authorized access to the computing facility and the IS. If uncleared or lower cleared personnel are employed, a fully cleared and technically qualified escort shall monitor and record all activities in a maintenance log. The level of detail required in the maintenance log is determined by the IAO. All maintenance personnel shall comply with DAA requirements for US citizenship, which are explicit for all classified systems.

13. Audit

a. Security Label Changes. GCCS-J shall support automatic recording of the creation, deletion, or changes in security labels, if security labeling is implemented.

b. Incident Response and Reporting. IAW CJCSI 6510.01D, GCCS-J shall provide for vulnerability mitigation and an incident response and reporting capability.

c. Collecting, Monitoring, and Reporting. An automated, continuous online monitoring and audit capability shall be deployed with the capability to alert personnel promptly of any unusual or inappropriate activity with potential security implications and to automatically disable the system if particularly serious security violations are detected.

d. Record Content. Audit records shall include all required information as directed in DODI 8500.2.

e. Audit Trail Protection. The contents of audit trails shall be protected against unauthorized access, modification, or deletion.

f. Audit Trail Backup. The audit records shall be backed up not less than weekly onto a different system or media than the system being audited. In addition, system audit records and system backups shall not be combined on the same media.

g. Audit Record Retention. Audit records shall be retained for the period specified in DODI 8500.2 (for PEL-4) with the ability for the records to be retrieved and create reports during that time (i.e., 2 years).

14. Session Controls

a. Inactivity. The system shall detect an interval of inactivity and block further access until the user reestablishes the connection using the proper validation.

b. Logon. Successive logon attempts shall be controlled using one or more of the following:

(1) Access is denied after multiple unsuccessful logon attempts.

(2) The number of access attempts in a given period is limited.

(3) A time-delay control system is employed. Further, if the system allows for multiple logon sessions for each user ID, the system shall provide a capability to control the number of logon sessions. Upon successful logon, the user shall be notified of the date and time of the user's last logon, the location of the user at last logon, and the number of unsuccessful logon attempts using this user ID since the last successful logon.

c. Warning Message. All users shall be warned that they are entering a government system and provided with the appropriate privacy and security statements, to include statements informing them that they are subject to monitoring, recording, and auditing. A Joint Staff legal advisor approved notice of privacy rights and security responsibilities shall be provided to all individuals attempting access to GCCS-J. GCCS-J shall ensure that appropriate warnings are provided to all individuals accessing GCCS-J information systems.

15. Environmental and Facilities

a. Temperature Controls. Automatic temperature controls shall be installed to prevent temperature fluctuations potentially harmful to personnel or equipment operation.

b. Fire Detection. The fire department shall receive an automatic notification of any activation of the smoke detection or fire suppression system.

c. Fire Suppression System. A fully automatic fire suppression system shall be installed that automatically activates when it detects heat, smoke, or particles.

d. Voltage Regulators. Automatic voltage control shall be implemented for GCCS-J devices (considered as critical IT assets). These devices include servers, any devices required to access the enclave (e.g., specific routers), and at least one workstation to manage the servers.

e. Emergency Lighting. An automatic emergency lighting system shall be installed covering all areas necessary to maintain full operations.

f. Humidity Controls. Automatic humidity controls shall be installed to prevent humidity fluctuations potentially harmful to personnel or equipment operation.

16. Security Testing

a. Functional and Integration Testing. At least one set of functional and integration testing shall be performed using the same security settings as those eused during certification testing to ensure the functionality delivered to the field performs with full security active. Certification testing shall be performed on GCCS-J and its strategic servers prior to each release for field use. Formal security test and evaluation shall be performed on the operational GCCS-J at least every 12 months. Each GCCS-J and strategic server accreditation delivery shall include independent testing by DIA as certifier of GCCS-J and its strategic servers. Each site GCCS-J DAA is responsible for the performance of local certification testing for any changes made to the type-accredited baseline for their site. GCCS-J, along with all GIG information systems, is subject to active penetrations and other forms of testing used to complement monitoring activities following DODD 4640.6 and other applicable laws and regulations. DIA can be requested to conduct vulnerability tests on the operational GCCS-J and its strategic servers. DISA staff may also perform their own vulnerability tests at the discretion of DISA. All findings resulting from DIA or DISA vulnerability tests will be coordinated with the site GCCS-J DAA or his designated representative within 24 hours of testing.

b. Compliance Testing. A comprehensive set of procedures testing all patches, upgrades, and new systems or applications prior to deployment into GCCS-J shall be implemented. Each field and site should assess whether the changes to the type baseline would be affected by or would affect field or site-unique changes. If field or site-unique changes affect or would be affected by the type baseline, then the field or site is responsible for implementing a comprehensive set of procedures testing all patches, upgrades, and new systems or applications differing from the type baseline prior to field or site deployment.

c. Assurance Mechanisms. A comprehensive certification test plan and process shall exist that requires testing, analysis, and documentation of each of the security functions of the system or site confirming they have no undesired effect(s) on the information being processed, that they perform as intended, and the system or site is operating following the established provisions and standards. The test methodology and procedures must be described in the test plan. In addition, an executable performance test schedule shall exist implementing the certification test plan. Performance testing shall incorporate a robust penetration testing process including periodic, unannounced in-depth monitoring of key systems and networks and providing for specific penetration testing to ensure compliance with all vulnerability mitigation procedures such as the DOD IAVA or other best security practices adopted or approved by the Department of Defense. Regular security performance testing is intended to ensure the system's security features continue to provide adequate assurance against constantly evolving threats and vulnerabilities. Independent validation and verification of the performance testing against the certification test plan and other requirements also should be conducted regularly.

d. Data Backup Testing. All GCCS-J sites shall test complete restoration of information from backup media at least quarterly.

e. Procedural Review. Conduct an annual security review that comprehensively evaluates existing policies and processes to ensure procedural consistency and to ensure they fully support the goal of uninterrupted operations.

f. Critical Utilities Testing. Arrangements for restoration of critical utilities to include long haul communications services shall be tested quarterly.

g. Physical Security. A facility penetration testing process shall be in place including periodic, unannounced attempts to penetrate key computing facilities.

h. Maintenance. A comprehensive maintenance testing process shall exist that systematically schedules critical hardware and peripheral equipment for periodic maintenance inspections and testing to ensure the equipment operates within design specifications and is properly calibrated.

ENCLOSURE C

RESPONSIBILITIES

1. Director, Joint Staff/J-6. Director, Joint Staff/J-6 serves as the global GCCS-J DAA and appoints a GSO.

a. Global GCCS-J DAA. The global GCCS-J DAA responsibilities include:

(1) Reviewing and approving security safeguards for the GCCS-J balancing the security safeguards against operational need.

(2) Issuing type accreditation statements based on the acceptability of the GCCS-J security safeguards against known risks and vulnerabilities.

(3) Approving GCCS-J site connections to non-GCCS-J systems. The global GCCS-J DAA must also approve connections between GCCS-J and systems of different security levels. Such connections also require approval from the DSAWG. Connections between GCCS-T and systems of lower security levels are prohibited.

(4) Ensuring all safeguards required, as stated in the GCCS-J type accreditation documentation, are implemented and maintained.

(5) Identifying security deficiencies and, where the deficiencies are serious enough to preclude type accreditation, taking action to achieve an acceptable security posture or accepting risk.

(6) Ensuring a GSO is named for the GCCS-J and that the GSO receives the necessary training to carry out the duties of this function.

(7) Requiring a GCCS-J security education, training, and awareness program must be in place.

(8) Ensuring information ownership is established for the GCCS-J, to include accountability, access rights, and special handling requirements.

(9) Establishing MOAs with DAAs of external, non-GCCS-J ISs connected to GCCS-J and site GCCS-J DAAs that have connections to external, non-GCCS-J ISs.

(10) Approving the security policy for GCCS-J.

(11) Ensuring a risk management plan is generated.

b. GSO. The GSO is the primary staff officer reporting to the global GCCS-J DAA. The GSO manages the GCCS-J security program. GSO responsibilities include:

(1) Implementing and managing the GCCS-J IS security program.

(2) Developing and maintaining the GCCS-J security policy and procedures.

(3) Implementing and managing the global GCCS-J DAA-approved security policy and procedures.

(4) Acting as the IS security advisor to the global GCCS-J DAA and providing security guidance to site GCCS-J IAOs.

(5) Reviewing all GCCS-J type, system, and site accreditation submissions and preparing accreditation recommendations for the global GCCS-J DAA.

(6) Serving as a voting member of the GCCS-J CMB as defined in CJCSI 6722.01A, "GCCS-J Configuration Management Policy." The GSO will have the primary responsibility for providing information to the CMB director on expected security impacts of all proposed system changes proposals submitted to the CMB.

(7) Maintaining this instruction and publishing amendments and changes as approved by the Joint Staff.

(8) Investigating and resolving security-related issues and incidents involving GCCS-J.

(9) Serving as Chairman of the GCCS Security Working Group.

(10) Ensuring GCCS-J sites, including strategic server sites, appoint site GCCS-J DAAs and IAOs in writing and maintain and publish an accurate list of appointees.

2. Site-Based Responsibilities

a. Site GCCS-J DAA. The site GCCS-J DAA responsibilities include:

(1) Reviewing and approving security safeguards for the site GCCS-J components.

(2) Issuing site accreditation statements based on the acceptability of deviations from the type-accredited GCCS-J baseline.

(3) Ensuring all required safeguards, as stated in the GCCS-J site accreditation documentation, are implemented and maintained.

(4) Identifying security deficiencies and, where the deficiencies preclude site accreditation, taking action to achieve an acceptable security posture.

(5) Requiring a site GCCS-J security education, training, and awareness program is in place.

(6) Ensuring information ownership is established for the site GCCS-J components, to include accountability, access rights, and special handling requirements.

(7) Establishing MOAs (MOUs if the DAA is the same for both components) with DAAs of external ISs and/or networks remotely connected to the site GCCS-J to ensure the continued security of sensitive information.

(8) Establishing MOAs with the global GCCS-J DAA when the GCCS-J components are connected to external non-GCCS-J systems.

(9) Approving GCCS-J site connections to non-GCCS-J SECRET systems, or TOP SECRET systems for GCCS-T, in coordination with the global GCCS-J DAA. The global must approve connections between GCCS-J and systems of different security levels. Connections between GCCS-T and systems of lower security levels are prohibited.

(10) Approving the GCCS-J site security policy.

(11) Ensuring all information system security incidents or violations are investigated and that appropriate corrective action is taken.

(12) Ensuring the site GCCS-J components are accredited for operational use.

(13) Ensuring the development and testing of site contingency plans.

(14) Reporting to Joint Staff/J-6 any site security anomalies that may adversely affect the GCCS-J network or servers.

(15) Ensuring a GCCS-J IAO and/or IAM is appointed in writing for the site; applicable training to carry out the duties of this function is received; and a proper organizational placement is established. (Assigning the site GCCS-J IAO or IAM to internal subordinate organizations hampers adequate security accomplishment and is therefore considered a security risk.)

(16) Ensuring a local GCCS-J Risk Management Program is implemented.

b. Site GCCS-J IAO. Reports to the site GCCS-J DAA and manages the site GCCS-J security program. Position requires a USG employee or person supervised by a USG employee (i.e., IAM) capable of ensuring GCCS-J security policy and guidance in this publication and other directives have been properly implemented. If a USG employee to whom the IAO directly reports is appointed the IAM, the IAO is not required to be a USG employee. The IAO is responsible for compliance with GCCS-J security procedures in an assigned area. IAOs may be assigned security responsibility for multiple workstations or areas as long as security is being maintained. If the IAO can logically maintain security control over multiple workstations in different rooms, then the intent of this requirement is met. The GCCS-J IAO responsibilities include:

(1) Ensuring maximum-security objectives are attained with minimum impact to mission requirements and operational performance.

(2) Developing, implementing, and managing the site GCCS-J IS security program, to include security education, training, and awareness.

(3) Developing and maintaining the site GCCS-J security policy and procedures.

(4) Coordinating and ensuring GCCS-J site certifications for GCCS-J.

(5) Functioning as the operational arm of the site GCCS-J DAA in implementing and managing the GCCS-J site-approved security policy and procedures.

(6) Acting as the site GCCS-J DAA IS security advisor in the absence of an IAM.

(7) Coordinating all GCCS-J site accreditation submissions and preparing accreditation recommendations for the site GCCS-J DAA.

(8) Monitoring the site GCCS-J equipment usage for unauthorized or improper activity through audit review and intrusion detection.

(9) Supervising and testing all site GCCS-J equipment and software changes.

(10) Investigating and reporting all GCCS-J site security violations to the site GCCS-J DAA, or Joint Staff/J-6 if outside the site's environment.

(11) Ensuring personnel who use the GCCS-J hold proper clearances and that access authorizations are current and valid.

(12) Performing periodic security audits of the GCCS-J.

(13) Performing password management.

(14) Ensuring written instructions specifying security requirements and operational procedures exist and are enforced.

(15) Implementing access management and other security-related functions within the scope of their assigned authorities.

(16) Reporting actual or suspected security deviations to the site IAM and/or DAA.

(17) Ensuring the workstations and network interfaces (hardware connections) are physically protected at the remote terminal area to the extent required for the sensitivity of information transmitted through the interfaces.

(18) Collecting and reviewing selected remote facility audit records, documenting any reported problems and corrective actions, and forwarding them to the DAA.

(19) Promoting security training and awareness.

(20) Acting as the trusted agent to the local registration authority to support GCSS users obtaining DOD PKI certificates.

3. Additional Security Support

a. Additional Roles. Besides the roles identified above, the site GCCS-J DAA and the GCCS-J IAO may appoint additional roles and responsibilities as necessary to implement an IS security program at their site. These may include but are not limited to GCCS-J IAMs, assistant IAOs, site coordinators, and site data base managers.

b. GCCS-J IAM. The GCCS-J IAM is assigned at the discretion of the site GCCS-J DAA for overall security management of single or multiple sites and/or IAOs. Position requires a USG employee capable of ensuring GCCS-J security policy is implemented and enforced. Experience in the application and enforcement of information and IS security measures, threats, and vulnerabilities is essential. Contractor personnel will not fill this position. Responsibilities include:

(1) Implementing security policy and providing security oversight of single or multiple sites and/or IAOs.

(2) Coordinating GCCS-J security measures including analysis, testing, evaluation, verification, accreditation, and review of GCCS-J installation at the appropriate classification level within the site's network structure.

(3) Ensuring security instructions, guidance, and SOPs are prepared and maintained at each site.

(4) Monitoring implementation of security guidance and directing action appropriate to remedy security deficiencies.

c. Other Roles. Other support roles such as alternate or assistant IAOs may be appointed as needed.

4. Defense Intelligence Agency. Supports the global GCCS-J DAA in the following manner:

a. Providing C&A services in support of GCCS-J baseline system type accreditation and strategic server system accreditation decisions.

b. Serving as the independent type certification authority for GCCS-J, its strategic servers, and GCCS-T.

c. Validating the minimum set of security requirements for safeguarding GCCS-J and GCCS-T information.

d. Independently validating security-relevant baseline changes to either the GCCS-J, GCCS-T, or strategic server configuration as well as corrections to previously identified security findings.

e. In concert with DISA, assessing and analyzing prototype system configurations for GCCS-J and GCCS-T computer security evaluations.

f. Using standard scanning tools approved by JTF-GNO (e.g., Gold Disk, Hercules, SCCVI) when evaluating the GCCS-J global and strategic server baseline security configurations to produce certification and/or security test and evaluation reports.

g. Conducting certification, test, and evaluation of type-baselines and strategic servers.

h. Reporting CT&E results with a recommendation to the GSO to support preparation of the GSO's accreditation recommendation to the global GCCS-J DAA.

i. Participating in GCCS CM to maintain awareness of baseline changes and to provide assessments of security-relevant changes.

5. Defense Information Systems Agency. DISA is the systems integration agent for GCCS-J. DISA responsibilities include:

a. Providing centralized security technical support for the development, maintenance, test, evaluation, and use of all components of GCCS-J.

b. Reviewing specifications for software and hardware security features.

c. In concert with DIA, providing support to Joint Staff/J-6 on security of software patches implemented between software releases.

d. Evaluating problem reports and change requests for security and providing results to the Joint Staff/J-6.

e. Evaluating GCCS-J security incident reports that deal with technical and system software issues and providing recommendations to the GSO.

f. In concert with DIA, participating in performing CT&Es on standard GCCS-J hardware and software as required by Joint Staff/J-6.

g. Developing, installing, analyzing, testing, and evaluating prototype IS security protection systems for GCCS-J with the appropriate Services, combatant commands, and Defense agencies.

h. Providing software tools and capabilities of declassifying and regrading standard GCCS-J hardware and removable media. Providing certification to the Joint Staff/J-6 that the software tools and capabilities perform as specified before field use and serving as its configuration manager. Providing a list of these software tools and capabilities to the GSO for further dissemination to site GCCS-J IAOs.

i. Supporting the GSO by maintaining technical cognizance of all aspects of computer network security, including hardware, software, COMSEC, and emanations security.

j. Evaluating specialized IA tools for use with GCCS-J.

k. Providing written mitigation plans for identified findings and vulnerabilities of GCCS-J to the GSO.

l. Evaluating and distributing standard automated software security tools to GCCS-J sites to support the GCCS-J IAO's implementation of this instruction as identified in CJCSI 6722.01, "GCCS-J Configuration Management Policy".

m. Reviewing and providing technical support for security procedures and measures.

n. Evaluating site-submitted software patches for operational effectiveness, security impact, etc.

o. Providing a technical analysis of security bulletins issued by organizations such as DOD-CERT, forum of incident response and security teams (FIRST), and operating systems (OS) developers that impact GCCS-J software.

p. Providing modifications to GCCS-J software in response to applicable security bulletins such as IAVAs and notices from CERT, FIRST, and OS developers.

q. Supporting GSO in ensuring the system certifications support sufficient testing for all hardware, software (operating systems and applications), and firmware in GCCS-J.

r. Providing and maintaining GCCS-J profile and policy for commercial security evaluation tools for the IAOs.

s. Load global GCCS-J DAA accepted vulnerabilities into the Vulnerability Management System (VMS) prior to fielding new releases.

t. Develop and maintain the GCCS-J SSAA for the type-accredited baseline and strategic servers.

6. GCCS-J User Security Responsibilities. Each GCCS-J user has security responsibilities contributing to the overall operational security of GCCS-J. GCCS-J users have the responsibility to be aware of and understand GCCS-J security. User responsibilities include:

a. Using the system for only authorized, official purposes.

b. Maintaining individual accountability, ensuring all operations are under assigned user account; not attempting to change or mask assigned user identity; and being responsible for all activity occurring under the assigned user account.

c. Changing access passwords as directed (minimum every 90 days), following local security SOPs provided by the site GCCS-J IAO. Protecting the SECRET password which authenticates the user by:

(1) Changing account password immediately after the first log in.

(2) Not permitting anyone else to use the assigned user account.

(3) Not revealing individual passwords to anyone else at any time.

(4) Storing SECRET passwords in authorized locations and/or containers.

d. Ensuring output products are marked or downgraded and properly safeguarded. Reporting unexpected or unrecognizable output to the GCCS-J IAO.

e. Not entering data of a higher classification level than the system (SECRET and TOP SECRET for GCCS-T).

f. Protecting classified and other sensitive material. Users will protect all system output (SECRET or TOP SECRET for GCCS-T) until reviewed as to actual classification (based on content) and appropriately downgraded by an approved process. All hardware and output will be marked (labeled) with applicable labels unless properly downgraded. Terminals and workstations located in their respective areas will be safeguarded.

g. Using only secure (SECRET and TOP SECRET for GCCS-T) communications links.

h. Not leaving GCCS-J terminals unattended and signed on.

i. Not moving hardware or altering communication connections without prior approval from appropriate local network configuration personnel. Maintaining minimum physical separation of system components following service red/black (TEMPEST) standards.

j. Checking all removable media for viruses before loading on GCCS-J.

k. Complying with all security guidance in this policy and in local security SOP.

l. Promptly reporting any system security abuses, abnormalities, discrepancies, incidents, vulnerabilities, or any other situation indicating inadequate security to the area security officer and the site GCCS-J IAO.

m. Operating the system reliably. The system will be used only as configured by the system administrator.

n. Not attempting to access files or data, or use operating systems, except as specifically designed or authorized.

o. Not installing any hardware or software (including importing or exporting of software). Only system administrators, with the GCCS-J IAO, can authorize and coordinate installation of additional software or hardware.

ENCLOSURE D

NETWORK SECURITY

1. System Identification, Need, and Mission Overview

a. DISA is leading the DOD effort to provide a modern, survivable, and secure DOD-wide network of computers, communications, and data applications that can evolve to meet user information requirements. This network initiative is driven by the DOD need for local and worldwide system interconnectivity, integration, and interoperability and encompasses the various systems supporting DOD missions and functions. Collectively, these systems are known as the defense information infrastructure (DII). The SIPRNET is one subset of the DII. The SIPRNET provides end-to-end information transfer and value-added services to transfer data up to the SECRET level. This policy does not replace any current security policy. SIPRNET security requirements also apply to any Service-unique networks or sub-networks used to transmit GCCS-J data. Detailed information for SIPRNET configuration, control, management, etc., can be found in the system and network management CONOPS, Defense Information Systems Network (DISN) CONOPS, and SIPRNET operations guide.

b. The SIPRNET architecture supports national defense command, control, communications, computers, and intelligence (C4I) worldwide information transfer requirements. The SIPRNET is the SECRET-level, router-based wide-area network (WAN) of the DISN. Before creation of the SIPRNET, the Department of Defense maintained the Defense Data Network (DDN) for DOD users worldwide. The DDN consisted of four packet-switched networks physically separated and identified according to the classification level of the data transported. The SECRET system high network portion of DDN was called Defense Systems Network 2 (DSNET2). In response to new technology and a changing subscriber base, DISN was established. The goal for DISN is to evolve into a worldwide information transfer infrastructure supporting long-haul requirements. SIPRNET was the first of the three DISN router layers to become operational under DISA. The SIPRNET supports those subscribers who were on the X.25 packet switching technology of the DDN DSNET2. SIPRNET will build on the following DISN initiatives for end-users systems:

(1) High-speed packet switching using Internet protocol routers (IPRs) and asynchronous switching using ATM switches.

(2) Circuit multiplexing using remotely managed smart multiplexers.

(3) Bundling access, trunk, and individual circuits for economies of scale.

(4) Integration and consolidation of network management and customer support.

c. The SIPRNET consists of routers, switches, hubs, communications servers, multiplexers, encryption devices, three regional control centers, one Global Control Center, one SIPRNET Support Center, a baseline of host connections, and the Integrated Tactical Strategic Demonstration Network (ITSDN). The ITSDN supports a DOD requirement to conduct two contingency operations in different parts of the world simultaneously. The ITSDN Quick Fix Program installed gateway routers to support deployed JTF contingencies, exercises, and training missions with requirements to interface with the DISN IPRs. Forces deployed using GCCS-J may rely on the ITSDN capabilities to reach the SIPRNET WAN. SIPRNET will provide high-speed software applications using IPRs. This high-speed datagram service is primarily intended to satisfy a large number of aggregated subscriber requirements coming from a multitude of LANs and WANs or subscriber premise routers. Subscriber connection requirements vary from those needing a sophisticated level of Internet routing support (such as complex subscriber domains with multiple routers, networks, and connections) to those needing a simple routing interface (such as a host). SIPRNET subscribers can be divided into four basic groups:

(1) Dedicated subscribers -- users on computers (mainframe hosts, PCs, or terminals) connected directly to the SIPRNET backbone routers via serial, Ethernet, and Fiber Distributed Data Interface lines and Synchronous Optical Network lines.

(2) Dial-up subscribers -- users who do not have the need for dedicated connections as well as temporary duty personnel. These users can access SIPRNET via approved COMSEC devices.

(3) Tactical subscribers -- users who gain access to the SIPRNET via the ITSDN. Tactical forces are allowed access to the SIPRNET, as well as other tactical networks via the Defense Satellite Communications

System, Global Broadcast Service, and MILSTAR through a standard tactical entry point.

(4) External network subscribers -- users on networks such as Air Force Network and Unclassified Internet Protocol Router Network (NIPRNET) who require access to the SIPRNET. Connections between UNCLASSIFIED and SECRET users are approved for UNCLASSIFIED e-mail only. Users can obtain a Secure Network Server that incorporates an approved guarding solution to facilitate the UNCLASSIFIED e-mail requirement.

d. GCCS-J local networks consist of routers, switches, hubs, communications servers, multiplexers, and encryption devices. This network of LANs and WANs connect GCCS-J users and non-GCCS-J users to the GCCS-J servers and/or the SIPRNET. The site GCCS-J DAA and site GCCS-J IAO ensure the security of the GCCS-J local networks and forward the accreditation to the GSO for approval. For those sites from which GCCS-J has been incorporated into the local backbone LAN structure, additional security enforcement must be provided to ensure GCCS-J does not experience a denial of service. Integrating GCCS-J into the local LAN structure increases the security management and implementation controls at the site not normally required if implemented as a separate network structure. Do not connect the GCCS-T LAN structures to any lower classified network until an NSA-approved multi-level security device is available, and the amended security policy is published by the Joint Staff.

2. Network Security Policy

a. The GCCS security policy is based upon DODD 8500.1, which establishes policy and assigns responsibilities to achieve DOD IA through a defense in depth approach that integrates the capabilities of personnel, operations, and technology and supports the evolution to network centric warfare. Director, DISA, is responsible for accrediting networks handling all general service data. Since SIPRNET is a subnet of the DISN, the DAA responsibilities are shared among the Directors of DISA, NSA, DIA, and Joint Staff.

b. GCCS-J Network Security Concept of Operations

(1) Compliance. SIPRNET and GCCS-J LAN users must follow the DISN security policy and applicable national, DOD, Service, and Defense agency security policies. In general, SIPRNET and the GCCS-J local network will process and protect all classified and sensitive information from unauthorized disclosure, modification, and destruction. The DISA responsibility ends at the encryption device and access circuit

connecting the subscriber's host, LAN, or premise router to the SIPRNET. SIPRNET connections will be accredited to operate at the security level of the corresponding network. These connections must never compromise SIPRNET security or integrity. GCCS-J-user information falls within the category covered by DODD C-5200.5, "Communications Security". As such, only NSA-endorsed products, techniques, and protected services will be used to protect SIPRNET access lines.

(2) GCCS-J LAN Configuration. A GCCS-J LAN has a GCCS-J management server and includes any connection to a network having a GCCS-J management server. It includes workstations connected to another network having a GCCS-J management server except when those connections are controlled by a STU-III secure device or a communications server requiring full I&A access.

(3) Confidentiality. DISA ensures the SIPRNET protects SECRET-level information and data in transit. In the case of GCCS-T, encryption devices will be used to prepare TOP SECRET data for transit at the SECRET-level over SIPRNET. SIPRNET and the GCCS-J local network will affect means necessary to prevent unauthorized information disclosure and/or dissemination.

(4) System Integrity. DISA will ensure controls are in place to prevent unauthorized SIPRNET and GCCS-J local network configuration modification.

(5) Data Integrity. Encryption provides the check used to ensure data integrity. SIPRNET, the GCCS-J local network, and the end system share responsibility for user data integrity. Generally, the end-user system is responsible for detecting and recovering information damaged or altered by the communication process through the transport service. However, SIPRNET bears total responsibility for network control data.

(6) Identification, Authentication, and Access Control. The SIPRNET does not have the capability to authenticate or control access for users of attached end systems. The end-user is responsible for I&A. SIPRNET and the GCCS-J local network will protect against external accesses to the information or system by encryption.

(7) Automated Nonrepudiation. Currently, SIPRNET and the GCCS-J local network do not provide an automated mechanism to show proof of origin such as digital signature. All proofs of origin must be determined through manual review of audit logs.

(8) Availability. SIPRNET and the GCCS-J local network will ensure uninterrupted user access to authorized functions and information.

(9) Network Security. Classified or sensitive information in clear text is not allowed to pass through the multiplexer layer or over individual circuits. All network devices, including IPRs, X.25 packet switches, X.500 asynchronous switches, multiplexers, and related components will be protected at the SECRET level. SIPRNET and GCCS-J local network users must protect all exposed trunks between IPR and X.25 packet switches and exposed subscriber access links to routers or switches with KG-type devices. The term exposed is defined as "exiting base, post, camp, or station boundaries."

(10) WEB Server Requirements. Management of Web servers will be strictly controlled at all sites. Password management, information content, gateway interfaces, and permission sets will be controlled to support maximum utility of the Web server while ensuring adequate security controls are in place. Public (unrestricted) access Web servers are to be isolated. Private Web servers, e.g., Web-enabled application servers, should be on dedicated systems and configured IAW DISA secure technical implementation guides. Each site should appoint an administrator to oversee Web server functions. The GCCS-J IAO may perform these functions.

(11) Enclaves. GCCS-J servers will be located in a GCCS-J enclave. Recommend GCCS-J clients are also located in the GCCS-J enclave. At a minimum, GCCS-J clients must be located in the local site, post, and/or station enclave.

3. Statements of Existing Accreditation and Waivers. DODD 8500.1 requires all DOD ISs be accredited. All SIPRNET users are required to have an accreditation document as a condition for granting SIPRNET access.

4. Disaster and Recovery Planning. Following DODI 8500.2, all SIPRNET and GCCS-J local network users are required to develop a disaster recovery plan, which includes a business recovery plan, system contingency plan, facility disaster recovery plan, and plan acceptance that provides for the smooth transfer of all mission or business essential functions to an alternate site for the duration of an event with little or no loss of operational continuity. Contingency plans must be tested to ensure IS security controls are effective and function reliably during service interruptions. DISA is responsible for all contingency planning for SIPRNET. The contingency plan must include recovery procedures

for modified or destroyed data. The contingency plan must address the following areas at a minimum:

a. Actions required if the normal communication environment is impaired or disrupted.

b. Actions required if the functional application is denied information or service (e.g., application cannot access needed information files or is denied service).

c. Users are denied information or service (e.g., user is denied application access).

d. Actions required for an emergency or expanded operations.

5. Configuration Management Requirements. DISA is responsible for overall SIPRNET CM. SIPRNET users will establish CM procedures to ensure changes made to their system's hardware, software, firmware, documentation, tests, test fixtures, and test documentation occur in an identifiable and controlled environment. System changes must never adversely affect SIPRNET properties or DISN security policy implementation.

6. Reports of Evaluated Products. Per DODD C-5200.5, only NSA-endorsed COMSEC products and services will be used to secure classified telecommunications of DOD components and their contractors. Only encryption devices listed in the Endorsed Cryptographic Products List of the *Information Systems Organization Products and Services Catalog* are authorized for use. These products have been endorsed for use in securing SECRET USG or government-derived information during its transmission. The DISN Program Management Office (PMO) provides all KG encryption technology as part of their service to the customer. SIPRNET users must provide their own encryption devices (e.g., STU-IIIs) for use within their network.

7. Organization and Resources. The Director, Joint Staff/J-6, through the DSAWG, will validate combatant command, Service, or Defense agency sub-networks for users requesting SIPRNET connectivity. Connectivity will normally be approved if residual risks not covered by SIPRNET mechanisms and procedures are sufficiently small and are outweighed by the operational benefits of network use.

ENCLOSURE E

GCCS-J SECURITY POLICY WAIVER AUTHORITY

1. Waiver Authority. The waiver authority for all requirements included in this document is the Joint Staff.

2. Waiver Requests. All requests for waivers must be sent to the Joint Staff/J-6X and Joint Staff/J-3/DDGO-CSOD in the form of an official memorandum signed by the site GCCS-J DAA. The memorandum should identify the requirement for which the waiver is requested; justification for the waiver; operational impact if the waiver is not granted; description of alternate solutions or procedures that will be implemented in place of the requirement; local points of contact; date by which the waiver is needed; and any supporting documentation that will assist the Joint Staff in making a decision.

3. Responses to Waiver Requests. The Joint Staff will respond, in writing, to all waiver requests.

(INTENTIONALLY BLANK)

ENCLOSURE F

GCCS STRATEGIC SERVER POLICY

1. This policy clarifies GCCS-J Security Policy in regards to certification and accreditation of GCCS-J strategic servers. GCCS-J is transitioning to a new architecture, placing global GCCS-J assets outside currently defined GCCS-J enclaves traditionally under combatant commander authority and control. Servers fitting within the definition of "GCCS-J strategic server" provide multiple combatant commanders access to global GCCS-J assets (e.g., JOPES, SORTS).

2. GCCS-J strategic servers will be treated as a component of GCCS-J following GCCS-J Security Policy. GCCS-J strategic servers are primarily operated and centrally managed by DISA as a GCCS-J site and provide worldwide access to GCCS-J data and services. DISA will follow defense agency responsibilities identified in this security policy.

3. To emphasize the proper certification, accreditation, and management processes of GCCS-J strategic servers, the following are highlighted for clarity:

a. Joint Staff/J-6, as global GCCS-J DAA, will provide "type" accreditation of GCCS-J strategic servers.

b. DIA, as the GCCS-J Certification Authority, will provide "type" certification of GCCS-J strategic servers.

c. The CM of GCCS-J strategic servers will follow GCCS-J CM Policy.

d. DISA, as site GCCS-J DAA for the GCCS-J strategic servers, will forward site accreditation documentation to global GCCS-J DAA. In addition, DISA will develop security documents (TFM, SFUG, etc.) for each strategic server baseline.

e. As the site GCCS-J DAA for the GCCS-J strategic servers, DISA is responsible for ensuring that an IAO or IAM is appointed to provide security guidance and support to site IAOs, resolve security issues (security incidents and sharing of cracked password reports), and conduct account reconciliation (twice a year).

(INTENTIONALLY BLANK)

ENCLOSURE G

GCCS PERSONAL DIGITAL ASSISTANT AND PERSONAL ELECTRONIC DEVICE POLICY

1. This enclosure establishes GCCS-J policy on PDAs and/or PEDs. It applies to all GCCS-J sites and personnel, including contractors, augmentees, and reservists assigned to or working within GCCS-J equipment locations. This policy memorandum applies to government-owned, contractor-supplied, or personally procured PDAs or PEDs as defined in paragraph 2.

2. PDAs, as referenced here, are small hand-held computing devices providing personal information management capability for users. PDA features include volatile and non-volatile memory, input capability, serial port, software modules, modem, and wireless data transfer capabilities. PEDs, as referenced here, are defined as hand-held electronic palm-top computers (e.g., Palm Pilot and/or similar items known by any other brand names), cellular phones, and pagers.

3. PDAs and PEDs are prohibited from processing GCCS-J information or accessing GCCS-J hardware or software. If GCCS-J classified information is loaded into a PDA or PED, the current means for declassification is destruction of the device. Report all incidents involving violation of this policy memorandum to the global GCCS-J DAA, Director, Joint Staff/J-6. Send incident reports via SIPRNET e-mail or secure fax within 24 hours of incident occurrence. Submit all requests for waivers or exceptions to this policy in writing to the global GCCS-J DAA for approval.

4. GCCS-J sites, local DAAs, and/or IAOs will educate personnel in GCCS-J workspaces on the guidance in this policy memorandum, report incidents to the global GCCS-J DAA, and confiscate, destroy, or sanitize equipment involved in security violations. Do not destroy equipment involved in security violations until investigation and, if warranted, disciplinary action is complete. All personnel assigned to or working within areas where GCCS-J equipment is located -- including contractors, augmentees, interagency or non-governmental personnel, and reservists -- will follow guidance in this policy.

(INTENTIONALLY BLANK)

ENCLOSURE H

GCCS-J KEYBOARD, VIDEO, MOUSE SWITCH POLICY

1. Introduction and Scope. This policy addresses life cycle management of peripheral switches used to connect GCCS-J hardware to systems operating at different security or sensitivity levels.

> Note: Any peripheral switch can be used, subject to site TEMPEST requirements, within the same classification or sensitivity level with the permission of the local DAA, but must be noted in the accreditation documentation and system security plan (SSP).

2. Definitions

a. Peripheral. A device such as, but not limited to, monitors, printers, keyboards, mice, and scanners. These devices may operate at the same or different classification levels.

b. KVM Switch. A mechanical or electrical switch connecting two or more computer systems to a single keyboard, video monitor, and mouse.

c. Printer or Scanner Switch. A mechanical or electrical switch connecting two or more computer systems to a single printer or scanner.

3. Policy

a. Only peripheral switches on the NSA Enterprise Solution baseline and/or DSAWG list of approved products shall be used when interconnecting GCCS-J hardware with systems of different classification or security levels.

b. DSAWG guidelines must be adhered to when using KVM switches to interconnect GCCS-J hardware with systems of different classification or security levels.

4. Requirements

a. To minimize the risk of inadvertently entering information onto the wrong system, the following requirements must be met:

(1) Labels. All GCCS-J components must be labeled following DCID 6/3, subparagraphs 8b2 (a and b). All switch positions, cables, and connectors shall be clearly marked with the appropriate classification labels.

(2) Training. The IAO shall train all personnel on using a peripheral switch, certify the user's training on a KVM switch user agreement, and retain the completed user agreement for record.

(3) Documentation. The SSPs and accreditation documentation for GCCS-J and all other systems connecting to the peripheral switch shall be updated to include the peripheral switch model number. Each switch installation will be accredited as a component of each attached system and will not change the attached system's protection level. Following DCID 6/3, each switch-connected system shall be re-accredited at least every 3 years.

b. For KVM peripheral switches only:

(1) Banners. The video monitor shall display a persistent security classification banner indicating the maximum classification of the system to which the KVM is actively attached. The classification banner shall display the maximum classification of the system in large bold type and its background color shall follow: Special compartmented information – Yellow; TOP SECRET – Orange; SECRET – Red; and UNCLASSIFIED – Green.

(2) Screen Lock. Screen lock applications shall display the maximum classification of the system executing and shall implement a lockout feature to re-authenticate users. Ensure each system's screen lock is invoked if there is a 5-minute period of inactivity.

(a) Smart Keys and Permanent Storage Medium. GCCS-J hardware using KVM switches shall not use "smart" or memory enhanced or data retaining keyboards, monitors, or mice, nor may they use wireless (i.e., infrared) mice or keyboards.

(b) Multiple Password Requirement. A different or unique password must be used for each system connected through the KVM switch.

(c) Shipment and Tamper Seals. All switches must be shipped to a central location that does not disclose the switches' final operational destination. If required for the specific switch, NSA protective technologies approved tamper seals shall be applied prior to the switches becoming operational.

(d) TEMPEST. Only use KVM switches in TEMPEST Zone C or Zone D facilities. Optical isolation or signal multiplexing will be required on all unclassified data connections using the KVM switch. Optical isolation and/or multiplexing shall be accomplished prior to the signal line leaving the controlled access area.

c. For printer or scanner peripheral switches only. When switching a printer or scanner between systems, complete the following steps in sequence:

(1) Power off the printer or scanner.

(2) Wait 10 seconds for the printer's or scanner's volatile memory to clear.

(3) Use the peripheral switch to select the desired computer.

(4) Power on the printer or scanner.

Note: If a computer loses track of the printer or scanner, it may be necessary to shut down and power up the computer. Printers or scanners that contain non-volatile memory (to include hard disk drives) must never be switched or interconnected between systems of different classification levels.

5. Responsibility

a. Local GCCS-J DAA. Ensure all authorizations for switches are obtained.

b. IAM/IAO

(1) Maintain the KVM switch user agreement files.

(2) Ensure each switch user receives the necessary training and follows the requirements for using peripheral switches.

(3) Ensure the systems are installed correctly and meet all applicable NSA/CSS TEMPEST standards.

(4) Update the GCCS-J SSPs and accreditation documentation to reflect the peripheral switch locations and model numbers.

(5) Ensure approved tamper seals are applied, if required, before the switches being installed.

c. User

(1) Protect the IS and peripherals located in their area.

(2) Report any spillage of classified information to the IAO and/or IAM.

(3) Safeguard and report any unexpected or unrecognizable computer output, including both displayed or printed products, following the GCCS-J System Security Policy, CJCSI 6731.01A.

(4) Use different passwords on each system connected through the KVM switch.

ENCLOSURE I

REFERENCES

The following documents are either included in this document or are helpful in executing this policy. These documents include executive orders; DOD directives, instructions, and standards; and CJCS instructions and manuals.

1. Executive Documents

a. Executive Order 12958, "Classified National Security Information"

b. Executive Order 12333, "United States Intelligence Activities"

c. Public Law 100-235, "The Computer Security Act of 1987"

d. OMB Circular No. A-130, "Management of Federal Information Resources"

e. OMB Circular No. A-123, "Management Accountability and Control"

f. Title 18, United States Code 1905, "Espionage Act," section 793, "Gathering, Transmitting, or Losing Defense Information", and section 794, "Gathering or Delivering Defense Information to Aid Foreign Government"

g. Information Security Oversight Office (ISOO) Directive No.1, "National Security Information"

h. Federal Register 32 CFR Part 2003, "National Security Information; Standard Forms; Final Rule", Part II ISOO

2. DOD and NSA Documents

a. Information Security

(1) DOD memorandum, 6 July 2006, "Interim Department of Defense Certification and Accreditation Process Guidance"

(2) DCID 6/3 Manual, "Protecting Sensitive Compartmented Information Within Information Systems"

(3) DODI 3200.14, 13 May 1997, "Principles and Operational Parameters of the DoD Scientific and Technical Information Program"

(4) DODD 5200.1, 13 December 1996, "DoD Information Security Program"

(5) DOD Regulation 5200.1-R, January 1997, "Information Security Program"

(6) DODD 5230.9, 9 April 1996, "Clearance of DoD Information for Public Release"

(7) DODD 5230.11, 16 June 1992, "Disclosure of Classified Military Information to Foreign Governments and International Organizations"

(8) DODD C-5230.23, 18 November 1983, "Intelligence Disclosure Policy (U)"

(9) DOD/ADUSD memorandum, "Interpretation of the Two-Person Integrity Requirement of Paragraph 7-100b", DOD 5200.1-R, "Information Security Program Regulation"

(10) DODI 7930.2, 31 December 1979, "ADP Software Exchange and Release"

(11) DOD 5220.22-M, February 2006, "National Industrial Security Program Operating Manual"

(12) DODD 5400.07, 29 September 1992, "DoD Freedom of Information Act (FOIA) Program"

(13) DODD 5400.11, 16 November 2004, "DoD Privacy Program"

(14) DODD 8500.1, 24 October 2002, "Information Assurance (IA)"

(15) DODI 8500.2, 6 February 2003, "Information Assurance (IA) Implementation"

(16) NSA, "Information Systems Security Products and Services Catalogue," published quarterly.

(17) SecDef memorandum, "Defense Acquisition"

b. Computer Security

(1) CSC-STD-003-85, "Computer Security Requirements"

(2) CSC-STD-004-85, "Technical Rationale Behind CSC-STD-003-85: Computer Security Requirements"

(3) NSTISSP No. 11, "National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products"

c. Operational Security

(1) DODD 5205.02, 6 March 2006, "DoD Operations Security (OPSEC) Program"

(2) DODD 5205.07, 5 January 2006, "Special Access Program (SAP) Policy"

(3) DODD 5205.8, 20 February 1991 (certified current as of 20 February 2004), "Access to Classified Cryptographic Information"

(4) DODD 5210.2, 12 January 1978 (incorporating through Change 3, 16 November 1994), "Access to and Dissemination of Restricted Data"

(5) DODD 5210.50, 22 July 2005, "Unauthorized Disclosure of Classified Information to the Public"

(6) DODD 5215.1, 25 October 1983, "Computer Security Evaluation Center"

(7) DODI 5215.2, 2 September 1986, "Computer Security Technical Vulnerability Reporting Program (CSTVRP)"

(8) DODD 3020.26, 8 September 2004, "Defense Continuity Program (DCP)"

d. Communications Security and Emissions

(1) DODD 4640.6, 26 June 1981, "Communication Security Telephone Monitoring and Recording"

(2) DODD C-5200.5, 21 April 1990, "Communications Security (COMSEC) (U)"

(3) DODD S-5200.17, 26 January 1965, "Security, Use and Dissemination of Communications Intelligence (COMINT) (U)"

(4) DODD C-5200.19, 16 May 1995, "Control of Compromising Emanations (U)"

(5) DODI 5210.74, 26 June 1985 (incorporating Change 1, 16 November 1994), "Security of Defense Contractor Telecommunications"

(6) DODI 5240.05, 22 February 2006, "Technical Surveillance Countermeasures (TSCM) Program"

(7) DOD C-5030.58-M, July 1978, "Defense Special Security Communications Systems, Security Criteria and Telecommunications Guidance (U)"

e. Personnel Security

(1) DODD 5200.2, 9 April 1999, "DoD Personnel Security Program"

(2) DOD Regulation 5200.2-R, January 1987, "Personnel Security Program"

(3) DODD 5220.6, 2 January 1992 (certified current as of 2 December 2003), "Defense Industrial Personnel Security Clearance Review Program"

f. Physical Security

(1) DODD 5200.8, 25 April 1991, "Security of DoD Installations and Resources"

(2) DODD 5220.22, 27 September 2004, "National Industrial Security Program"

(3) DOD Regulation 5220.22-R, December 1985, "Industrial Security Regulation"

(4) DOD Manual 5220.22-M, 28 February 2006, "National Industrial Security Program Operating Manual"

g. Web Security

(1) DepSecDef memorandum, 24 September 1998, "Information Vulnerability and the World Wide Web"

(2) DepSecDef memorandum, 7 December 1988, "Web Site Administration"

(3) ASD(C3I) document, 25 November 1988, "Web Site Administration Policies and Procedures"

3. CJCS Instructions and Manuals

a. CJCSM 3122.01, "Joint Operation Planning and Execution System (JOPES) Volume I (Planning Policies and Procedures)"

b. CJCSM 3122.03 Series, "Joint Operation Planning and Execution System Volume II Planning Formats and Guidance"

c. CJCSM 3150.02, "Global Status of Resources and Training System"

d. CJCSI 3137.01 Series, "The Functional Capabilities Board Process"

e. CJCSI 3213.01 Series, "Joint Operations Security"

f. CJCSM 3213.02 Series, "Joint Staff Focal Point Communications Procedures Manual (U)"

g. CJCSI 5714.01 Series, "Police for the Release of Joint Information"

h. CJCSI 6211.02 Series, "Defense Information System Network (DISN): Policy, Responsibilities and Processes"

i. CJCSI 6212.01 Series, "Interoperability and Supportability of Information Technology and National Security Systems"

j. CJCSI 6215.01 Series, "Policy for Department of Defense Voice Networks"

k. CJCSI 6510.01 Series, "Information Assurance (IA) and Computer Network Defense (CND)"

l. CJCSI 6721.01 Series, "Global Command and Control Management Structure"

m. CJCSM 6721.01 Series, "Global Command and Control Systems-Joint (GCCS-J) Functional Requirements Evaluation Procedures"

n. CJCSI 6722.01 Series, "Global Command and Control System Configuration Management Policy"

4. Standards. International Organization for Standardization (ISO) 9000.

GLOSSARY
PART I - ABBREVIATIONS AND ACRONYMS

The following acronyms and their abbreviations may not appear in the instruction but are commonly used within the GCCS-J security environment.

ADP	automated data processing
AFNET	Air Force Network
ATM	asynchronous transfer mode
C2	command and control
C4I	command, control, communications, computers, and intelligence
C&A	certification and accreditation
CAP	connection approval package
CC	common criteria
CCDR	combatant commander
CCB	Configuration Control Board
CERT	computer emergency response team
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CJCSM	Chairman of the Joint Chiefs of Staff Manual
CJTF	commander, joint task force
CM	configuration management
CMB	Configuration Management Board
COE	common operating environment
COMSEC	communications security
CONOPS	concept of operations
COTS	commercial off-the-shelf
C/S/A	combatant command, Service, or agency
CSS	Central Security Service
CT&E	certification test and evaluation
DAA	designated approving authority
DCID	Director, Central Intelligence Directive
DDA	designated development activity
DDGO/CSOD	Deputy Directorate for Global Operations, Command Systems Operations Directorate (Joint Staff/J-3)
DDN	Defense Data Network
DIA	Defense Intelligence Agency
DII	defense information infrastructure
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DISR	DOD Information Technology Standards

DNS	domain name service
DOD	Department of Defense
DODD	Department of Defense Directive
DODI	Department of Defense Instruction
DSAWG	DISN Security Accreditation Working Group
DSCS	Defense Satellite Communications System
DSNET2	Defense Secure Network 2
EMSEC	emanations security
EPL	evaluated products list
FDDI	fiber distributed data interface
FIRST	forum of incident response and security teams
GBS	Global Broadcast Service
GCC	Global Control Center
GCCS-J	Global Command and Control System-Joint
GCCS-T	Global Command and Control System –Top Secret
GENSER	general service
GIG	Global Information Grid
GMC	GCCS Management Center
GMC/NOC	GMC/Network Operations Center
GOTS	government off-the-shelf
GSO	GCCS-J security officer
I&A	identification and authentication
IA	information assurance
IAM	information assurance manager
IAO	information assurance officer
IATFF	information assurance technical framework forum
IAVA	information assurance vulnerability alert
IAW	in accordance with
IDS	intrusion detection system
IP	Internet protocol
IPR	Internet protocol router
ISSE	information systems security engineer
IS	information system
IT	information technology
ITSDN	Integrated Tactical Strategic Demonstration Network
IVV	independent validation and verification
J-3	operations directorate of a joint staff
J-6	command, control, communication and computers systems directorate of a joint staff
JCAT	joint crisis action team

JC2	joint command and control
JFRG	joint force requirements generator
JTF	joint task force
JTF-GNO	Joint Task Force – Global Network Operations
JOPES	Joint Operation Planning and Execution System
JSSC	joint staff support center
KG	keystream generator
KVM	keyboard, video, mouse
LAN	local area network
LCM	life-cycle management
MAC	mandatory access control
MILSTAR	military strategic and tactical relay system
MLS	multilevel security
MOA	memorandum of agreement
MOU	memorandum of understanding
NCSC	National Computer Security Center
NCSC-TG	NCSC-technical guide
NDP	national disclosure policy
NES	network encryption system
NIPRNET	Non-Secure Internet Protocol Router Network
NIST	National Institute of Standards and Technology
NOC	network operations center
NSA	National Security Agency
NSTISSP	National Security Telecommunications and Information Systems Security Policy
NT	New Technology
OMB	Office of Management and Budget
OS	operating system
PDA	personal digital assistant
PED	personal electronic device
PKE	public key encryption
PKI	public key infrastructure
PMO	program management office
RA	risk analysis
RCC	regional control center
RFI	radio frequency interference
ROM	read-only memory

S/W	software
SFUG	security features user's guide
SIOP	secure identification operating procedure
SIPRNET	SECRET Internet Protocol Router Network
SMG	standard mail guard
SNMP	simple network management protocol
SNS	secure network server
SOA	service oriented architecture
SONET	synchronous optical network
SOP	standard operating procedure
SORTS	Status of Resources and Training System
SPECAT	special category
SSC	SIPRNET support center
SSP	system security plan
SSTM	single service training manager
STD	standard
STEP	standard tactical entry point
STIG	secure technical implementation guide
ST&E	security test and evaluation
STU-III	secure telephone unit III
SW	software
TCB	trusted computing base
TCSEC	trusted computer system evaluation criteria
TFM	trusted facility manual
USERID	user identification
USG	US government
VMS	Vulnerability Management System
WAN	wide-area network

PART II – DEFINITIONS

NOTE: Terms marked with "*" are not standardized within the Department of Defense and are applicable only in the context of this document.

access* -- 1. A specific type of interaction between a subject (i.e., a person, process, or input device) and an object (i.e., an IS resource such as a record, file, program, or output device) that results in the transfer of information. 2. The ability and opportunity to obtain knowledge of classified or sensitive but unclassified information.

accountability* -- The property that enables activities on an IS to be traced to individuals who may then be held responsible for their actions.

accreditation* -- A formal declaration by the designating approval authority (DAA) having accreditation responsibility that the information system (IS) is approved to operate in one or more particular security modes using a prescribed set of safeguards. Accreditation is the official management authorization for operation of an IS and is based on the certification process and on other management considerations. The accreditation statement affixes security responsibility with the DAA and shows that due care has been taken for security.

information system security* -- Measures and controls required to protect against unauthorized (accidental or intentional) disclosure, modification, or destruction of information systems (ISs) and data and denial of service to process data. IS security includes consideration of all hardware and software functions, characteristics, or features; operational procedures, accountability procedures, and access controls at the central computer facility, remote computer, and terminal facilities; management constraints; physical structures and devices; and personnel and communications controls needed to provide an acceptable level of risk for the IS and for the data and information contained in the system. The totality of security safeguards needed to provide an acceptable protection level for an IS and for data processed by an IS.

assurance* -- A measure of confidence that the security features and architecture of an information system (IS) accurately implement, mediate, and enforce the security policy. If the security features of an IS are relied upon to process sensitive information and restrict user access, the features must be tested to ensure that the security policy is enforced during IS operation.

asynchronous transfer mode (ATM)* -- An emerging technology that can transmit multi-media (digitized voice, video, and data) across local, metropolitan, and wide-area networks. ATM is an international standard defined by American National Standards Institute and International

Telecommunications Union – Telecommunications Standards Sector that implements a high speed, connection-oriented, cell switching and multiplexing technology designed to provide users with virtually unlimited bandwidth.

audit* -- To conduct an independent review and examination of system records and activities to test for adequacy of system controls to ensure compliance with established policy and operational procedures and recommend changes in controls, policy, or procedures.

audit trail* -- A set of collective records that documents evidence of processing used to trace from original transactions forward to related records and reports and/or backwards from records and reports to their component source transactions.

authenticate -- 1. To verify the identity of a user, device, or other entity in a computer system, often as a prerequisite to allowing access to resources in the system. 2. To verify the integrity of data that have been stored, transmitted, or otherwise exposed to possible unauthorized modification.

browsing -- The act of searching through storage to locate or acquire information without necessarily knowing of the existence or the format of the information being sought. (NCSC-TG-004, Version 1)

classification authority -- The authority vested in a DOD official to make an initial determination that information requires protection against unauthorized disclosure in the interest of national security. (DOD 5200.1-R)

classification guide -- A document issued by an authorized original classifier that prescribes the level of classification and appropriate declassification instructions for specified information to be classified derivatively. (DOD 5200.1-R)

closed security environment* -- An environment in which the following conditions hold true: (1) Application developers (including maintainers) have sufficient clearances and authorizations to provide an acceptable presumption that they have not introduced malicious logic; (2) Configuration control provides sufficient assurance that applications and the equipment are protected against the introduction of malicious logic prior to and during the operation of systems applications.

commercial off-the-shelf software* -- Software acquired by government contract through a commercial vendor. This software is a standard product, not developed by a vendor for a particular government project.

communications security (COMSEC) -- The protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from the possession and study of telecommunications. COMSEC includes crypto security, transmission security, emission security, and physical security of COMSEC materials and information.

a. crypto security -- The component of COMSEC that results from the provision of technically sound cryptosystems and their proper use.

b. transmission security -- The component of COMSEC that results from all measures designed to protect transmissions from interception and exploitation by means other than crypto analysis.

c. emission security -- The component of COMSEC that results from all measures taken to deny unauthorized persons information of value that might be derived from intercept and analysis of compromising emanations from crypto-equipment and telecommunications systems.

d. physical security -- The component of COMSEC that results from all physical measures necessary to safeguard classified equipment, material, and documents from access thereto or observation thereof by unauthorized persons.

compromise* -- A violation of security policy of a system such that unauthorized disclosure of sensitive information occurred.

compromising emanations* -- Unintentional data-related or intelligence-bearing signals that, if intercepted and analyzed, disclose the information transmission received, handled, or otherwise processed by any information processing equipment.

communications security (COMSEC) equipment* -- Equipment designed to provide security to telecommunications by converting information to a form unintelligible to an unauthorized interceptor and by reconverting such information to its original form for authorized recipients as well as equipment designed specifically to aid in, or as an essential element of, the conversion process. COMSEC equipment is crypto-equipment, crypto-ancillary equipment, crypto-production equipment and authentication equipment.

computer security -- Synonymous with automated information security. (NCSC-TG-004, Version 1)

confidentiality level -- Applicable to DOD information systems, the confidentiality level is primarily used to establish acceptable access factors, such as requirements for individual security clearances or background investigations, access approvals, and need-to-know determinations; interconnection controls and approvals; and acceptable methods by which users may access the system (e.g., intranet, Internet, wireless). The Department of Defense has three defined confidentiality levels: classified, sensitive, and public. (DODI 8500.2, February 6, 2003)

configuration control -- The process of controlling modifications to the system's hardware, firmware, software, and documentation that provides sufficient assurance that the system is protected against the introduction of improper modifications prior to, during, and after system implementation. Compare configuration management. (NCSC-TG-004, Version 1)

configuration management -- The management of security features and assurances through control of changes made to a system's hardware, software, firmware, documentation, test, test fixtures, and test documentation throughout the development and operational life of the system. Compare configuration control. (NCSC-TG-004, Version 1)

countermeasure -- Any action, device, procedure, technique, or other measure that reduces the vulnerability of, or threat to, a system. (NCSC-TG-004, Version 1)

data* -- A representation of facts, concepts, information, or instructions suitable for communication, interpretation, or processing by humans or by an information system.

data integrity* -- The state that exists when datum is unchanged from its source and accidentally or maliciously has not been modified, altered, or destroyed.

data owner* -- The authority, individual, or organization that has original responsibility for the data by statute, executive order, or directive.

declassification -- The determination that, in the interests of national security, classified information no longer requires any degree of protection against unauthorized disclosure, coupled with removal or cancellation of the classification designation. (Joint Pub 1-02)

declassification (of information system magnetic storage media)* -- A procedure that will totally remove all the classified or sensitive information stored on magnetic media followed by a review of the procedure performed. A decision can then be made for (or against) actual removal of the classification level of the media. Declassification allows release of the media from the controlled environment if approved by the appropriate authorities.

defense in depth* -- The proposition that multiple layers of security are better than a single protection mechanism. The layers may be technological, procedural, or policy.

defense information infrastructure* -- The capability within the Department of Defense for local and worldwide system interconnectivity, integration, and interoperability for the various systems that support the DOD missions and functions.

degauss -- Destroy information contained in magnetic media by subjecting that media to high intensity alternating magnetic fields, following which, the magnetic fields slowly decrease. (NCSC-TG-025)

denial of service* -- Action or actions that result in the inability of an information system or any essential part to perform its designated mission, either by loss or degradation of operational capability.

designated approving authority -- The official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. This term is synonymous with designated accrediting authority and delegated accrediting authority. (DODD 8500.1)

designated development activity* -- The activity assigned responsibility by Joint Staff/J-6 for development of a Global Command and Control System-Joint standard software capability.

discretionary access control -- A means of restricting access to objects based on the identity and need to know of the user, process, and groups to which they belong. The controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject. Compare mandatory access control. (NCSC-TG-004, Version 1)

downgrade -- To determine that classified information requires, in the interests of national security, a lower degree of protection against unauthorized disclosure than currently provided, coupled with a changing of the classification designation to reflect such lower degree. (Joint Pub 1-02)

downgrading (of magnetic storage media) -- A procedure used under the system high (e.g., TOP SECRET) mode of operation that will reclassify the magnetic storage media to reflect the true (actual) classification of classified or sensitive information stored. (NCSC-TG-025) emanations security* -- Also called EMSEC. The protection that results from all measures designed to deny unauthorized person's information of value that might be derived from intercept and analysis of compromising emanations.

enclave -- Collection of computing environments connected by one or more internal networks under the control of a single authority and security policy, including personnel and physical security. Enclaves always assume the highest mission assurance category and security classification of the IS applications or outsourced IT-based processes they support, and derive their security needs from those systems. They provide standard IA capabilities, such as boundary defense, incident detection and response, and key management, and deliver common application, such as office automation and electronic mail. Enclaves are analogous to general support systems as defined in OMB A-130. Enclaves may be specific to an organization or a mission, and the computing environments may be organized by physical proximity or by function independent of location. Examples of enclaves include local area networks and the applications they host, backbone networks, and data processing centers. (DODI 8500.2)

evaluated products list -- A documented inventory of equipment, hardware, software, or firmware that has been evaluated against the evaluation criteria.

external system exposure -- A measure of the degree of isolation from other information systems, either through physical or cryptographic means. (DODI 8500.2)

fiber distributed data interface* -- An American National Standards Institute-defined standard specifying a 100-megabytes per second token-passing network using fiber-optic cable. Uses a dual-ring architecture to provide redundancy.

firmware* -- Software that is permanently stored in a hardware device that allows reading of the software but not writing or modifying. The most common device for firmware is read-only memory.

gateway* -- A device or system that enables the passage of data between networks.

Global Command and Control System (GCCS) Management Center/Network Operations Center* -- A center that operates 24 hours a day within the Pentagon and constantly monitors network status and coordinates network operations. This network coordination center supports the activities of the National Military Command Center, GCCS-Joint (GCCS-J) security officers, and GCCS-J users.

Global Broadcast Service* -- A new high-speed multimedia satellite communication technology.

group account* -- A user identification shared by more than one authorized user. Also implies sharing of the associated SECRET password.

individual accountability -- The ability to associate positively the identity of a user with the time, method, and degree of access to a system. (NCSC-TG-004, Version 1)

information security* -- The system of policies, procedures, and requirements established under the authority of executive orders or statutes to protect information that, if subjected to unauthorized disclosure, could reasonably be expected to cause damage to the national security.

information system -- Set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information.

information systems security* -- A composite means of protecting telecommunications systems and automated information systems and the information they process.

integrity -- Quality of an information system reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. Note that, in a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information. (DODD 8500.1)

internal system exposure -- A measure of the difference between the established security criteria for individual access and the actual access privileges of authorized users. (DODI 8500.2, February 6, 2003)

least privilege* -- The principle that requires that each subject be granted the most restrictive set of privileges needed for the performance of authorized tasks. The application of this principle limits the damage that can result from accidents, error, or unauthorized use.

local area network* -- A short-haul data communications system that connects information system devices in a command or base structure, including (but not limited to) workstations, front-end processors, controllers, switches, and gateways.

mandatory access control* -- A means of restricting access to objects based on the sensitivity (as requested by a label) of the information contained in the objects and the formal authorization (i.e., clearance) of subjects to access information of such sensitivity.

multilevel security* -- Concept of processing information with different classifications and categories that simultaneously permits access by users with different security clearances but prevents users from obtaining access to information for which they lack authorization.

need to know -- Necessity for access to, or knowledge or possession of, specific official DOD information required to carry out official duties. (DODD 8500.1)

network* -- A communications medium and all components attached to that medium whose responsibility is the transference of information. Such components may include information systems, packet switches, telecommunications controllers, key distribution centers, and technical control devices.

non-repudiation -- Assurance that the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data. (DODD 8500.1)

object -- A passive entity that contains or receives information. Access to an object potentially implies access to the information it contains. Object examples are records, blocks, pages, segments, files, directories, directory trees, and programs, as well as bits, bytes, words, fields, processors, video displays, keyboards, clocks, printers, network nodes. (NCSC-TG-004, Version 1)

object reuse -- The reassignment and reuse of a storage medium (e.g., page frame, disk sector, magnetic tape) that once contained one or more objects. To be securely reused and assigned to a new subject, storage media must contain no residual data (magnetic remanence) from the object(s) previously contained in the media. (NCSC-TG-004, Version 1)

open security environment -- An environment that includes those systems in which at least one of the following conditions holds true: (1) Application developers (including maintainers) do not have sufficient clearance or authorization to provide an acceptable presumption that they have not introduced malicious logic. (2) Configuration control does not provide sufficient assurance that applications are protected against introduction of malicious logic prior to and during the operation of system applications. (NCSC-TG-004, Version 1) operating system* -- An integrated collection of service routines for supervising the sequencing and processing of programs by a computer. Operating systems control the allocation of resources to users and their programs and play a central role in assuring the secure operation of a computer system. Operating systems may perform input or output accounting, resource allocation, storage assignment tasks, and other system-related functions (synonymous with monitor, executive, control program, and supervisor).

operational performance data (network)* -- A measure of the effectiveness of the SIPRNET as seen by a user in relationship to job performance. Typically expressed in terms of success rate (with regard to job completion; e.g., transferring a file or accessing an application in a server or client), speed of service (system responsiveness or time required to complete a job), and accuracy.

output-only devices* -- Devices, such as printers, connected to a server or client (directly or through communications devices) that perform no input functions to the server or client.

overwrite -- A procedure to remove or destroy data recorded on magnetic storage media by writing patterns of data over or on top of the data stored on the media. (NCSC-TG-025)

password -- A protected or private character string used to authenticate an identity. (NCSC-TG-004, Version 1)

penetration* -- The successful act of bypassing the security mechanisms of a system.

penetration testing* -- The portion of security testing in which the penetrators attempt to circumvent the security features of a system. The penetrators may be assumed to use all system design and implementation documentation, which may include listings of system source code, manuals, and circuit diagrams. The penetrators work under no constraints other than those that would be applied to ordinary users.

periods processing* -- A manner of operating an information system (IS) in which the security mode of operation and/or maximum classification of data processed by the IS is established for an interval of time or period and then changed for the following interval of time. A period extends from any secure initialization of the IS to the completion of any purging of sensitive data processed by the IS during the period.

public domain software* -- Software acquired from government or non-government sources, often at no charge, when the source takes no responsibility for the integrity or maintenance of the software.

purge* -- Removal of sensitive data from an information system (IS) at the end of a period of processing, from IS storage devices and other peripheral devices with storage capacity, so there is assurance proportional to the sensitivity of the data that the data may not be reconstructed. An IS must be disconnected from any external network before a purge.

read access -- Permission to read information. (NCSC-TG-004, Version 1)

read-only memory (ROM)* -- A storage area in which the contents can be read but not altered during normal computer processing.

recovery procedures* -- The actions necessary to restore a systems computational capability and data files after a system failure.

regrade -- To determine that certain classified information requires, in the interest of national defense, a higher or a lower degree of protection against unauthorized disclosure than currently provided, coupled with a changing of the classification designation to reflect such higher or lower degree. (Joint Pub 1-02)

residue -- Data left in storage after processing operations are complete, but before degaussing or rewriting has taken place. (NCSC-TG-004, Version 1)

risk* -- A combination of the likelihood that a threat shall occur, the likelihood that a threat occurrence shall result in an adverse impact, and the severity of the resulting adverse impact.

risk analysis* -- An analysis of system assets and vulnerabilities to establish an expected loss from certain events based on estimated probabilities of occurrence.

risk analysis -- The process of identifying security risks, determining their magnitude, and identifying areas needing safeguards. Risk analysis is a part of risk management. Synonymous with risk assessment. (NCSC-TG-004, Version 1)

risk management -- The total process of identifying, controlling, and eliminating or minimizing uncertain events that may affect system resources. It includes risk analysis, cost-benefit analysis, selection, implementation and test, security evaluation of safeguards, and overall security review. (NCSC-TG-004, Version 1) root access* -- A function or state in which a user or program has unrestricted access to the operating system, applications programs, or data, whether in memory or on media.

sanitize -- To erase or overwrite classified data stored on magnetic media for the purpose of declassifying the media. (NCSC-TG-025)

SECRET* -- The unauthorized disclosure of this information or material could reasonably be expected to cause serious damage to the national security.

SECRET Internet Protocol Router Network (SIPRNET) -- A subset of the defense information infrastructure that provides end-to-end information transfer and value-added services for the transport of data up to the SECRET level. The SIPRNET architecture supports national defense command, control, communications, computers, and intelligence worldwide information transfer requirements. It is a router-based wide area network of the Defense Information Systems Network. It consists of routers, hubs, communications servers, multiplexers, encryption devices, switches, three regional control centers, one Global Control Center, and one SIPRNET Support Center.

security incident* -- An incident involving classified information in which there is a deviation from the requirements of governing security regulations (e.g., compromise, inadvertent disclosure, need-to-know violation, and administrative deviation).

security mode* -- A mode of operation in which the designated approving authority accredits an information system (IS) to operate. Inherent with each of the four security modes (dedicated, system high, multilevel, partitioned) are restrictions on the user clearance levels, formal access requirements, need-to-know requirements, and the range of sensitive information permitted on the IS.

security-relevant event* -- Any event that attempts to violate the security policy of the system (e.g., too many attempts to logon).

security test and evaluation -- An examination and analysis of a system's security safeguards as they have been applied in an operational environment to determine the security posture of the system. (NCSC-TG-004, Version 1)

service level agreement* -- A contract between a network service provider and a customer that specifies, usually in measurable terms, what services the network service provider will furnish. It includes defined minimum performance measures at or above which the service delivered is considered acceptable.

site accreditation* -- Official authentication by the site designating approval authority to employ a system in a specified environment. This authorization includes a statement of residual risk and delineates operating environment and specific use. It is performed when multiple copies of a system are to be fielded.

synchronous optical network* -- An emerging network that will eventually allow asynchronous transfer mode to be deployed at rates of 622 megabytes per second, 1.2 gigabytes per second, and 2.4 gigabytes per second.

system access* -- 1. Users' capability to logon to a computer system or network. 2. Access privileges given to maintainers of the operating system files.

system accreditation* -- The accreditation of a major system application, general support system, or a clearly defined independent system.

system users* -- Those individuals with direct connections to the system and those without direct connections that receive output or generate input that is not reliably reviewed for classification by a responsible individual. The clearance of system users is used in the calculation of risk index.

TEMPEST -- The study and control of spurious electronic signals emitted by electrical equipment. (NCSC-TG-004, Version 1)

threat -- Any circumstance or event with the potential to cause harm to a system in the form of destruction, disclosure, modification of data, and/or denial of service. (NCSC-TG-004, Version 1)

TOP SECRET -- The unauthorized disclosure of this information or material could reasonably be expected to cause exceptionally grave damage to the national security.

Trojan Horse* -- A computer program with an apparently or actually useful function that contains additional "hidden" functions that surreptitiously exploit the legitimate authorizations of the invoking process to the detriment of security or integrity.

trusted computing base (TCB)* -- The totality of protection mechanisms within a computer system, including hardware, firmware, and software, the combination of which is responsible for enforcing a security policy. A TCB consists of one or more components that together enforce a unified security policy over a product or system. The ability of a TCB to correctly enforce a unified security policy depends solely on the mechanisms within the TCB and on the correct input by system administrative personnel of parameters (e.g., a user's clearance level) related to the security policy.

trusted path* -- A mechanism by which a person at a terminal can communicate directly with the trusted computing base (TCB). This mechanism can be activated only by the person of the TCB and cannot be imitated by software that is not trusted.

type accreditation* -- Evaluates a common application or system that is distributed to a number of different locations.

user* -- A person who interacts directly with client or server system. In Global Command and Control System-Joint (GCCS-J), a person or organization that has access to GCCS-J through a client or that is allowed to submit input to the system through other media (e.g., tape or floppy disk) and has been assigned an individual or group USERID and password. (Does not include those persons or organizations defined as customers.)

virus* -- A self-propagating Trojan horse composed of a mission component, a trigger component, and a self-propagating component.

vulnerability -- A weakness in system security procedures, system design, implementation, internal controls, etc., that could be exploited to violate system security policy. (NCSC-TG-004, Version 1) Vulnerability is also the susceptibility of a particular system to a specific attack, along with the opportunity available to a hostile entity to mount that attack. A vulnerability is always demonstrable, but may exist independently of a known threat. In general, a description of a vulnerability takes account of those factors under friendly control.

workstation* -- Typically, a workstation has an operating system such as Universal Network Information Exchange (UNIX) that is capable of running several tasks at the same time. It typically has several megabytes of memory and a large, high-resolution display. Personal computers have increased significantly in power and capability and can be potentially on par with some UNIX platforms. For joint systems, UNIX platforms and personal computers are referred to generically as workstations.

write access* -- Permission to write to an object.

(INTENTIONALLY BLANK)